Anne Riechert
Oskar-von-Miller-Str. 20
60314 Frankfurt

Dissertation

„Neue Online-Dienste und Datenschutz am Beispiel von Virtuellen Privaten Netzwerken“

Prof. Dr. Peter Wedde
Fachhochschule Frankfurt
Nibelungenplatz 1
60318 Frankfurt

Prof. Dr. Wolfgang Däubler
Universität Bremen
Bibliothekstraße 1
28359 Bremen

Vorwort

Der Fachbereich der Rechtswissenschaft der Universität Bremen hat die vorliegende Arbeit im November 2006 als Dissertation angenommen.

Mein besonderer Dank gilt:

Herrn Prof. Dr. Peter Wedde und Herrn Prof. Dr. Wolfgang Däubler, die diese Arbeit betreuten und die Gutachten erstellten. Vor allem das Motto „Es gibt immer eine Lösung“ (Prof. Dr. Peter Wedde) wird mir in besonderer Erinnerung verbleiben und ist nicht nur für andere Doktoranden mehr als empfehlenswert.

Darüber hinaus gebührt mein Dank ebenso Herrn Dr. Peter Stumpf für seine fortwährende Unterstützung und meinen Eltern, die mir den Weg zum Studium ermöglichten.

Anne Riechert

Gliederung

Literaturverzeichnis

Abel, Horst G.:
Praxishandbuch Datenschutz, Das Standardwerk für den öffentlichen und nicht-öffentlichen Bereich, Band1, Stand: September 2006, Kissing

Abel, Horst G.:
Praxishandbuch, IT-Know-how für den Datenschutzbeauftragten, Rechtssichere Beurteilung von Netzwerken, Datenbanken und E-Mail-Systemen, Stand: März 2004, Augsburg

Akmann, Torsten:
Nationale Überwachung als Baustein europäischer Sicherheit, in:
Holznagel Bernd / Nelles, Ursula / Sokol, Bettina, Die neue TKÜV (Telekommunikationsüberwachungsverordnung), in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 27, München 2002

Albrecht, Rüdiger:
Die Einrichtung von Tele- und Außenarbeitsplätzen – Rechtliche und personalpolitische Anforderungen, NZA 1996, S. 1240 ff.

Altenhein, Karsten:
Die gebilligte Verbreitung missbilligter Inhalte – Auslegung und Kritik des § 5 Teledienstegesetz, AfP 1998, S. 457 ff.

Altenburg, Stephan / v. Reinersdorff, Wolfgang / Leister, Thomas:
Telekommunikation am Arbeitsplatz, MMR 2005, S. 135 ff.

Altenburg, Stephan / v. Reinersdorff, Wolfgang / Leister, Thomas:
Betriebsverfassungsrechtliche Aspekte der Telekommunikation am Arbeitsplatz, MMR 2005, S. 222 ff.

Antoine, Ludwig:
IP-Adresse als „andere Kennung“ eines TK-Anschlusses, ITRB 2004, S. 56

Antoine, Ludwig:
Unterlassungsanspruch gegen Spam, ITRB 2004, S. 11

Auernhammer, Herbert:
Bundesdatenschutzgesetz, Kommentar, 3. Auflage, Köln, u.a. 1993

Backu, Frieder:
Pflicht zur Verschlüsselung?, Gefahren und Konsequenzen der unverschlüsselten E-Mail-Kommunikation, ITRB 2003, S. 251 ff.

Bär, Wolfgang:
Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100g, 100 h StPO, MMR 2002, S. 358 ff.

Barta, Thomas / Klöcker, Irene / Meister, Jörg:
Datenschutz im Krankenhaus, 2. Auflage, Düsseldorf 2001

Barton, Dirk, M.:
(Mit-) Verantwortlichkeit des Arbeitgebers für rechtsmissbräuchliche Online-Nutzungen durch den Arbeitnehmer, Findet die Haftungsprivilegierung des §9 Abs. 1 TDG auch auf den Arbeitgeber Anwendung? CR 2003, S. 592 ff.

Barton, Dirk, M.:
E-Mail-Kontrolle durch Arbeitgeber, Drohen unliebsame strafrechtliche Überraschungen?, CR 2003, S. 839 ff.

Baum, Michael / Trafkowski, Armin:
Verschlüsselung und Strafzumessung, CR 2002, S. 69 ff.

Bäumler, Helmut:
Das TDDSG aus Sicht eines Datenschutzbeauftragten, DuD 1999, S. 258 ff.

Bäumler, Helmut:
Datenvermeidung und Datensparsamkeit, in: Baeriswyl, Bruno / Rudin, Beat (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, S. 351 ff., Zürich 2002

Beckschulze, Martin:
Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz – Rechte der Beteiligten und Rechtsfolgen bei Pflichtverletzungen - , DB 2003, 2777 ff.

Beheim, Johannes:
Sicherheit von Vertraulichkeit bei europaweiter Mobilkommunikation, Zellulare Digital-Mobilfunksysteme D900 und D1800 bieten sicheren Informationsschutz über GSM-Standards hinaus, DuD 1994, S. 327 ff.

Bergmann, Lutz / Möhrle, Roland / Herb, Armin:
Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und Kirchen sowie zum Bereichsspezifischen Datenschutz, 31.Ergänzungslieferung, Dezember 2004/2005, Stuttgart u.a. 2005

Bettinger, Torsten / Freytag, Stefan:
Privatrechtliche Verantwortlichkeit für Links, CR 1998, S. 545 ff.

Bettinger, Torsten / Scheffelt, Michael:
Application Service Providing: Vertragsgestaltung und Konflikt-Management, CR 2001, S. 729 ff.

Beucher, Klaus / Leyendecker, Ludwig / Rosenberg, Oliver von (Hrsg.):
Mediengesetze, Rundfunk, Mediendienste, Teledienste, Kommentar zum Rundfunkstaatsvertrag, Mediendienstestaatsvertrag, Teledienstegesetz und Teledienstedatenschutzgesetz, München 1999

Bier, Sascha:
Internet und Email am Arbeitsplatz, DuD 2004, S. 277 ff.

Bijok, Bernd-Christoph / Class, Thomas:
Arbeitsrechtliche und datenschutzrechtliche Aspekte des Internet-Einsatzes (insbesondere E-Mail), RDV 2001, S. 52 ff.

Bischof, Elke / Witzel, Michaela:
Softwarepflegeverträge, Inhalte und Problemstellungen, ITRB 2003, S. 31 ff.

Bizer, Johann:
Gateway, DuD 2000, S. 44 ff.

Bizer, Johann:
Verpflichtung zur Herausgabe von TK-Verbindungsdaten an den Staatsanwalt, DuD 2002, S. 237 ff.

Bizer, Johann:
Web-Cookies – datenschutzrechtlich, DuD 1998, S. 277 ff.

Bizer, Johann:
Private Internetnutzung am Arbeitsplatz, DuD 2004, S. 432

Bizer, Johann:
Das Recht der Protokollierung, DuD 2006, S. 270 ff.

Bleisteiner, Stephan:
Rechtliche Verantwortlichkeit im Internet, Köln, u.a. 1999

Blümel, Markus / Soldo, Erwin:
Internet-Praxis für Juristen, Online-Einstieg leicht gemacht, Köln, u.a. 1998

Boemke, Burkhard / Ankersen, Per:
Das Telearbeitsverhältnis – Arbeitsschutz, Datenschutz und Sozialversicherungsrecht, BB 2000, S. 1570 ff.

Boemke, Burkhard / Ankersen, Per:
Telearbeit und Betriebsverfassung, BB 2000, S. 2254 ff.

Böhmer, Wolfgang:
VPN, Virtual Private Networks, Die reale Welt der virtuellen Netze, München 2002

Böhmer, Wolfgang:
VPN, Virtual Private Networks, Kommunikationssicherheit in VPN- und IP-Netzen über GPRS und WLAN, 2. Auflage, München, u.a. 2005

Bonin, Andreas von / Köster, Oliver:
Internet im Lichte neuer Gesetze, ZUM 1997, S. 821 ff.

Bothe, Michael / Heun, Sven-Erik / Lohmann, Torsten:
Rechtsfragen des Errichtens und Betreibens von Fernmeldeanlagen, Archiv Telekommunikation 1995, S. 5 ff.

Bräutigam, Peter / Leupold, Andreas (Hrsg.):
Online-Handel, Betriebswirtschaftliche und rechtliche Grundlagen, Einzelne Erscheinungsformen des E-Commerce, München 2003

Breinlinger, Astrid:
Die Kontrolle des Datenschutzbeauftragten aus Sicht der Aufsichtsbehörden, RDV 1995, S. 7 ff.

Brühann, Ulf:
EU-Datenschutzrichtlinie – Umsetzung in einem vernetzten Europa, RDV 1996, S. 12 ff.

Büchner, Wolfgang / Ehmer, Jörg / Geppert, Martin / Kerkhoff, Bärbel / Piepenbrock, Hermann-Josef / Schütz, Raimund / Schuster, Fabian (Hrsg.):
Beck`scher TKG-Kommentar, 2. Auflage, München 2000 (zitiert: Bearbeiter in: TKG-Kommentar (2. Auflage))

Buckbesch, Jörg / Köhler, Rolf-Dieter:
VPN, Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, Köln 2001

Bücking, Jens:
Namens- und Kennzeichenrecht im Internet (Domainrecht), Stuttgart, u.a. 1999

Büllesbach, Alfred / Rieß, Joachim:
Outsourcing in der öffentlichen Verwaltung, NVwZ 1995, S. 444 ff.

Büllesbach, Alfred:
Das TDDSG aus Sicht der Wirtschaft, DuD 1999, S. 263 ff.

Büllesbach, Alfred:
Datenschutz bei Data Warehouse und Data Mining, CR 2000, S. 11 ff.

Büllesbach, Alfred:
Finanzdatenschutz in Europa, CR 2000, S. 544 ff.

Büllingen, Franz:
Vorratsdatenspeicherung von Telekommunikationsdaten im internationalen Vergleich, DuD 2005, S. 349 ff.

Campo, Markus / Pohlmann, Norbert:
Virtual Private Networks, 2. Auflage, Bonn 2003

Cichon, Caroline:
Internetverträge: Verträge über Internet-Leistungen und Ecommerce, Köln 2000

Cichon, Caroline:
Internetverträge: Verträge über Internet-Leistungen und Ecommerce, 2. Auflage Köln 2005

Czychowski, Klaus / Bröcker, Tim:
ASP – Ein Auslaufmodell für das Urheberrecht?, MMR 2002, S. 81 ff.

Dammann, Ullrich / Rabenhorst, Klaus:
Outsourcing und Auftragsdatenverarbeitung, CR 1998, S. 643

Däubler, Wolfgang:
Das Fernsprechgeheimnis des Arbeitnehmers, CR 1994, S. 754 ff.

Däubler, Wolfgang:
Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht, NZA 2001, S. 874 ff.

Däubler, Wolfgang:
Internetnutzung am Arbeitsplatz – Kontrolle durch den Arbeitgeber ?, Arbeit – Umwelt, Joachim Heilmann zum 60. Geburtstag, Festschrift Joachim Heilmann, S. 1 ff., 1. Auflage, Baden-Baden 2001;

Däubler, Wolfgang:
Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht, NZA 2001, S. 874 ff.

Däubler, Wolfgang:
Nutzung des Internet durch Arbeitnehmer, K&R 2000, S. 323 ff.

Däubler, Wolfgang:
Internet und Arbeitsrecht, 3. Auflage, Frankfurt am Main 2004

Däubler, Wolfgang:
Gläserne Belegschaften?, Datenschutz in Betrieb und Dienststelle, 4. Auflage, Frankfurt am Main 2002

Däubler, Wolfgang / Kittner, Michael / Klebe, Thomas (Hrsg):
BetrVG, Betriebsverfassungsgesetz mit Wahlordnung und EBR-Gesetz, 10. Auflage, Frankfurt am Main 2006 (zit.: Bearbeiter in: Däubler/Kittner/Klebe, BetrVG)

Davis, Carlton, A.:
IPSEC, Tunneling im Internet, Bonn 2002

Degenhart, Christoph
Die allgemeine Handlungsfreiheit des Art. 2 Abs. 1 GG, JuS 1990, S. 161 ff.

Deutsche Postgewerkschaft (Hrsg.):
Basisinformation Telearbeit, Frankfurt am Main 1998 (zitiert: Basisinformation Telearbeit des Projekts „Online-Forum Telearbeit“)

Dick, Andreas:
Rundum-Sorglos-Paket oder Alptraum auf Raten, ASP, S. 41 ff., Application Service Providing Magazin, Nov./Dez., 6/2000

Dieselhorst, Jochen:
Sperrungsverfügung gegenüber Access-Provider, ITRB 2003, S. 194 ff.

Dieterich, Thomas / Preis, Ulrich / Müller-Glöge, Rudi / Schaub, Günter(Hrsg.):
Erfurter Kommentar zum Arbeitsrecht, 5. Auflage, München 2005 (zitiert: Bearbeiter in: Erfurter Kommentar)

Dilger, Petra:
Verbraucherschutz bei Vertragsabschlüssen im Internet, in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreiche Information und Recht, Band 32, München 2002

Dix, Alexander:
Vorratsspeicherung von IP-Adressen?, Anmerkungen zur Bewertung der Praxis von der T-Online International AG durch das Regierungspräsidium Darmstadt, DuD 2003, S. 234 ff.

Dix, Alexander / Gardain, Anja-Maria:
Datenexport in Drittstaaten, Neue Wege zur Gewährleistung ausreichender Schutzgarantien, DuD 2006, S. 343 ff.

Dolderer, Günter /v.Garrel, Gerd / Müthlein, Thomas / Schlumberger, Peter:
Die Auftragsdatenverarbeitung im neuen BDSG, RDV 2001, S. 223 ff.

Dornseif, Maximilian / Schumann, Kay, H. / Klein, Christian:
Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke, DuD 2002, S. 226 ff.

Dörr, Dieter:
Die Entwicklung des Medienrechts, NJW 1995, S. 2263 ff.

Dreier, Horst
Grundgesetz Kommentar, Band I, Präambel Art. 1-19, 2. Auflage, Tübingen 2004 (zitiert: Bearbeiter in: Dreier, GG-Kommentar)

Dück, Peter:
Sobald Anwendungen selbst Billing-Komponenten enthalten, können ASPs über noch flexiblere Preis-Modelle in Wettbewerb treten, ASP, S. 23 ff., Application Service Providing Magazin, Nov./Dez., 6/2000,

Eberle, Carl-Eugen / Rudolf, Walter / Wasserburg, Klaus (Hrsg.):
Mainzer Rechtshandbuch der Neuen Medien, Heidelberg 2003

Eckhardt, Jens:
Datenschutz und Überwachung im Regierungsentwurf zum TKG, CR 2003, S. 805 ff.

Eckhardt, Jens:
Neue Regelungen der TK-Überwachung, DuD 2002, S. 197

Eckhardt, Jens:
Telekommunikations-Überwachungsverordnung – Ein Überblick, CR 2001, S. 670 ff.

Eckhardt, Jens:
Wie weit reicht der Schutz des Fernmeldegeheimnisses (Art. 10 GG)?, DuD 2006, S. 365 ff.

Ehmann, Eugen / Helfrich, Marcus:
EG Datenschutzrichtlinie, Kurzkommentar, Köln 1999

Eichhorn, Bert:
Internet-Recht, Ein Lehrbuch für das Recht im Word-Wide-Web, 2. Auflage, Köln 2001

Ellinghaus, Ulrich:
Erste Stufe der TKG-Novelle: Umsetzung des TK-Richtlinienpakets durch Zeitablauf, Eine Analyse zu Art und Umfang der unmittelbaren Wirkung des TK-Richtlinienpakets, CR 2003, S. 657 ff.

Ellinghaus, Ulrich:
TKG-Novelle und Europarecht: Probleme mit der Flexibilisierung, Eine Analyse der Umsetzung europarechtlicher Vorgaben zur Marktregulierung im Regierungsentwurf, CR 2004, S. 23 ff.

Engel, Christoph:
Die Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden, Eine Kritik an den Verfügungen der Bezirksdirektion Düsseldorf, MMR-Beilage 4/2003, S. 1 ff.

Engel-Flechsig / Maennel, Frithjof, A. / Tettenborn, A.:
Das neue Informations- und Kommunikationsdienste-Gesetz, NJW 1997, S. 2981 ff.

Engel-Flechsig, Stefan / Maennel, Frithjof, A. / Tettenborn, Alexander (Hrsg.):
Beck´scher IuKDG-Kommentar, München 2001 (zitiert: Beck-IuKDG-Bearbeiter)

Engel-Flechsig, Stefan:
Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer – Einheitliche Rahmenbedingungen für Multimedia, ZUM 1997, S. 231 ff.

Engel-Flechsig, Stefan:
Die datenschutzrechtlichen Vorschriften im neuen Informations- und Kommunikationsdienste-Gesetz, RDV 1997, S. 59 ff.

Engel-Flechsig, Stefan:
Die neue Medienordnung, in:
Bartsch, Michael / Lutterbeck, Bernd (Hrsg.), Neues Recht für neue Medien, Köln 1998 S. 61 ff.

Engel-Flechsig, Stefan:
Teledienstedatenschutz, DuD 1997, S. 8 ff.

Engels, Stefan / Eimterbäumer, Elke:
Sammeln und Nutzen von e-Mail-Adressen zu Werbezwecken, K&R 1998, S. 196 ff.

Enzmann, Matthias / Scholz, Philipp:
Technisch-organisatorische Gestaltungsmöglichkeiten, in:
Roßnagel, Alexander (Hrsg.), Datenschutz beim Online-Einkauf, S. 73 ff., Braunschweig/Wiesbaden 2002

Ernst, Stefan:
Der Arbeitgeber, die E-Mail und das Internet, NZA 2002, S. 585 ff.

Ernst, Stefan:
Wireless LAN und das Strafrecht, Zur Strafbarkeit des „Abhörens“ ungesicherter Kommunikation, CR 2003, S. 898 ff.

Ernst, Stefan:
Privates Surfen am Arbeitsplatz als Kündigungsgrund, DuD 2006, S. 223 ff.

Evers, Jürgen / Kiene, Lorenz H.:
Die Wirksamkeitskriterien von Einwilligungsklauseln und die Auslagerung von Finanzdienstleistungen im Sinne des § 11 BDSG, NJW 2003, S. 2726 ff.

Evers, Jürgen / Kiene, Lorenz H.:
Auslagerung von Finanzdienstleistungen auf Handelsvertreter: Anforderungen an die Einwilligungserklärung hinsichtlich der Weitergabe von Kundendaten, DB 2003, S. 2762 ff.

Evertz, Stephan:
Arbeitsrecht, in: Schwerdtfeger, Armin / Evertz, Stephan / Kreuzer, Philipp, Amadeus / Peschel-Mehner, Andreas / Poeck, Torsten / (Hrsg.), Cyberlaw, S. 55 ff., Wiesbaden 1999

Fasbender, Andreas:
Schwachstellen der Informationsverarbeitung durch Dritte, RDV 1994, S. 12 ff.

Fechner, Frank:
Medienrecht, Lehrbuch des gesamten Medienrechts unter besonderer Berücksichtigung von Presse, Rundfunk und Multimedia, 7. Auflage Tübingen 2006

Fedderath, Hannes / Thees, Jürgen:
Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern, DuD 1995, S. 338 ff.

Federrath, Hannes:
Schwachstelle Schnittstelle: Angriffspunkt für Datenspione, in: Holznagel Bernd / Nelles, Ursula / Sokol, Bettina, Die neue TKÜV (Telekommunikationsüberwachungsverordnung), S. 115 ff., in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 27, München 2002

Feldmann, Thorsten:
Etappensieg für die Bezirksregierung Düsseldorf im Streit um Website-Sperrung, ITRB 2003, S. 118 ff.

Feldmann, Thorsten:
Website-Sperrung in NRW vorerst gestoppt, ITRB 2003, S. 22 ff.

Fickert, Tim / Nau, Matthias / Gerling, Rainer, W.:
Encrypting File System unter Windows, Features, Lücken, Gefahren, Vorteile, DuD 2003, S. 223 ff.

Fischer, Ulrich / Schierbaum, Bruno:
Telearbeit und Datenschutz, Eine vernachlässigte Debatte, CR 1998, S. 321 ff.

Fitting, Karl:
Betriebsverfassungsgesetz mit Wahlordnung, Handkommentar, 3. Auflage, München 2006

Fleck, Ulrike:
Brauchen wir ein Arbeitnehmerdatenschutzgesetz, BB 2003, S. 306 ff.

Fox, Dirk:
Der IMSI-Catcher, DuD 2002, S. 212 ff.

Freytag, Stefan:
Haftung im Netz, Verantwortlichkeit für Urheber-, Marken- und Wettbewerbsrechtsverletzungen nach § 5 TDG und § 5 MDStV, in: Hoeren, Thomas / Spindler, Gerald, Holznager, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, München 1999

Freytag, Stefan:
Urheberrechtliche Haftung im Netz, Zur dogmatischen Einordnung und praktischen Umsetzung von § 5 TDG und § 5 MDStV bei Urheberrechtsverletzungen im Internet, ZUM 1999, S. 185 ff.

Fröhle, Jens:
Web Advertising, Nutzerprofile und Teledienstedatenschutz, in:
Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert / Dreier, Thomas (Hrsg.), Schriftenreiche Information und Recht, Band 42, München 2003

Galperin, Hans / Löwisch, Manfred:
Kommentar zum Betriebsverfassungsgesetz, 6. Auflage, Heidelberg 1982

Geiger, Andreas:
Die Einwilligung in die Verwendung von persönlichen Daten aus Ausübung des Rechts auf informationelle Selbstbestimmung, NVwZ 1989, S. 35 ff.

Geis, Ivo:
Das neue Datenschutzrecht für Teledienste, CR 2002, S. 667 ff.

Geis, Ivo:
Recht im eCommerce, Elektronische Geschäfte und Internetpräsenz zuverlässig absichern, Neuwied, u.a. 2001

Geis, Ivo:
Schutz von Kundendaten im E-Commerce und elektronische Signatur: RDV 2000, S. 208 ff.

Geis, Ivo:
Internet und Datenschutzrecht, NJW 1997, S. 288 ff.

Gennen, Klaus:
Outsourcing und §631a BGB, ITRB 2002, S. 291 ff.

Geppert, Martin / Piepenbrock, Hermann-Josef / Schütz, Raimund / Schuster, Fabian (Hrsg.):
Beck`scher TKG-Kommentar, 3. Auflage, München 2006 (zitiert: Bearbeiter in: TKG-Kommentar (3. Auflage))

Geppert, Martin / Ruhle, Ernst-Olav / Schuster, Fabian:
Handbuch Recht und Praxis der Telekommunikation, 2. Auflage, Baden-Baden 2002

Geppert, Martin / Ruhle, Ernst-Olav / Schuster, Fabian:
Handbuch Recht und Praxis der Telekommunikation, Baden-Baden 1998

Gerling, Rainer W.:.
IT-Sicherheit und Datenschutz, Ein Widersprich?, DuD 2005, S. 338 ff.

Glatt, Christoph:
Vertragsschluss im Internet, Unter besonderer Berücksichtigung der Rechtsentwicklung in der Europäischen Union und des internationalen Verbrauchervertrages, Baden-Baden 2002

Globig, Klaus / Eiermann, Helmut:
Datenschutz bei Internet-Angeboten, DuD 1998, S. 514 ff.

Gnirck, Karen / Lichtenberg, Jan:
Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen, DuD 2004, S. 598 ff.

Göckel, Andreas:
Internet Domain-Namen: Die Entwicklung der Rechtssprechung in Deutschland, in: Königshofen, Thomas (Hrsg.), Das neue Telekommunikationsrecht in der Praxis, S. 126 ff., Heidelberg 1999

Gola, Peter:
Datenschutz und Multimedia am Arbeitsplatz, 1. Auflage, Frechen 2006

Gola, Peter:
Die Entwicklung des Datenschutzrechts im Jahre 1995/96, NJW 1996, S. 3312f.

Gola, Peter / Klug, Christoph:
Die Entwicklung des Datenschutzrechts in den Jahren 2000/2001, NJW 2001, S. 3747 ff.

Gola, Peter / Klug, Christoph:
Grundzüge des Datenschutzrechts, München 2003

Gola, Peter / Müthlein, Thomas:
Neuer Tele-Datenschutz – bei fehlender Koordination über das Ziel hinausgeschossen?, RDV 1997, S. 193 ff.

Gola, Peter / Müthlein, Thomas:
TDG, TDDSG: Teledienstegesetz, Teledienstedatenschutzgesetz, Kommentierung für die Praxis, Frechen 2000

Gola, Peter / Schomerus, Rudolf:
BDSG, Bundesdatenschutzgesetz, Kommentar, 8. Auflage, München 2005

Gola, Peter / Wronka, Georg:
Werbung, Wettbewerb und Datenschutz, RDV 1994, S. 157 ff.

Gola, Peter, Jaspers, Andreas:
Datenschutz bei Telearbeit – Zur Anwendung von BDSG, TKG und TDDSG – RDV 1998, S. 243 ff.

Gola, Peter:
Die Entwicklung des Datenschutzrechts im Jahre 1998/1999, NJW 1999, S. 3753 ff.

Gola, Peter:
Die Entwicklung des Datenschutzrechts in den Jahren 1999/2000, NJW 2000, S. 3749 ff.

Gola, Peter:
Neuer Tele-Datenschutz für Arbeitnehmer?, Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MMR 1999, S. 322 ff.

Gounalakis, Georgios / Rhode, Lars:
Elektronische Kommunikationsangebote zwischen Telediensten, Mediendiensten und Rundfunk, CR 1998, S. 487 ff.

Gounalakis, Georgios / Rhode, Lars:
Persönlichkeitsschutz im Internet, Grundlagen und Online-Spezifika, München 2002

Gounalakis, Georgios:
Der Mediendienste-Staatsvertrag der Länder, NJW 1997, S. 2993 ff.

Gounalakis, Georgios (Hrsg.):
Rechtshandbuch Electronic Business, München 2003 (zitiert: Bearbeiter in: Gounalakis, Rechtshandbuch Electronic Business)

Grote, Elisabeth:
Die Telekommunikations-Kundenschutzverordnung, Neue Rechtslage für Kundenbeziehungen im Telekommunikationsgeschäft, BB 1998, S. 1117 ff.

Grützmacher, Malte:
Application Service Providing – Urhebervertragsrechtliche Aspekte IT-Recht kompakt 2001 S. 59 ff.

Gundermann, Lukas:
E-Commerce trotz oder durch (-235)Datenschutz?, K&R 2000, S. 225 ff.

Haft, Fritjof / Eisele, Jörg:
Zur Einführung: Rechtsfragen des Datenverkehrs im Internet, JuS 2001, S. 112 ff.

Hamm, Rainer / Hammer, Volker:
Kritische IT-Infrastrukturen: DuD 2003, S. 240 ff.

Hamm, Rainer:
TKÜV – ein Kompromiss auf dem Boden der Verfassung?, in: Holznagel Bernd / Nelles, Ursula / Sokol, Bettina, Die neue TKÜV (Telekommunikationsüberwachungsverordnung), S. 81 ff., in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 27, München 2002

Hanau, Peter / Hoeren, Thomas / Andres, Dirk:
Private Internetnutzung durch Arbeitnehmer - Die arbeits- und betriebsverfassungsrechtlichen Probleme-, in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert / Dreier, Thomas (Hrsg.), Schriftenreiche Information und Recht, Band 34, München 2003 (zitiert: Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer)

Harte-Bavendamm, Henning / Henning-Bodewig, Frauke (Hrsg.):
Gesetz gegen den unlauteren Wettbewerb (UWG), Mit Preisangabenverordnung, Kommentar, München 2004

Härting, Niko:
Die Gewährleistungspflichten von Internet-Dienstleistern, CR 2001, S. 37 ff.

Haupt, Susanne / Wollenschläger, Michael:
Virtueller Arbeitsplatz – Scheinselbständigkeit bei einer modernen Arbeitsorganisationsform, NZA 2001, S. 289 ff.

Hefermehl, Wolfgang / Köhler, Helmut / Bornkamm, Joachim:
Wettbewerbsrecht, Gesetz gegen den unlauteren Wettbewerb, Preisangabenverordnung, Band 13 a, 24. Auflage, München 2006

Heidrich, Joerg:
Die T-Online-Entscheidung des RP Darmstadt und ihre Folgen, DuD 2003, S. 237 ff.

Heidrich, Joerg / Tschoepe, Heidrich:
Rechtsprobleme der E-Mail-Filterung, MMR 2004, S. 75 ff.

Hellmich, Stefanie:
Location Based Services – Datenschutzrechtliche Anforderungen, MMR 2002, S. 152 ff.

Herzog, Marco:
Rechtliche Probleme einer Inhaltsbeschränkung im Internet, in:
Gornig, Gilbert (Hrsg.), Schriften zum internationalen und zum öffentlichen Recht, Band 39, Frankfurt am Main u.a. 2000

Hess, Harald / Schlochauer, Ursula / Worzalla, Michael / Glock, Dirk:
BetrVG, Kommentar zum Betriebsverfassungsgesetz , 6. Auflage, München 2003 (zitiert: Bearbeiter in: Hess/Schlochauer/Worzalla/Glock)

Heyl, Cornelius von:
Teledienste und Mediendienste nach Teledienstegesetz und Mediendienste-Staatsvertrag, ZUM 1998, S. 115 ff.

Heymann, Thomas:
Outsourcing als Form der Kooperation, CR 2000, S. 23 ff.

Hilber, Marc, D. / Frik, Roman:
Rechtliche Aspekte der Nutzung von Netzwerken durch Arbeitnehmer und den Betriebsrat, RdA 2002, S. 89 ff.

Hilger, Herbert:
Zulässigkeit der Telefondatenerfassung, DB 1986, S. 911 ff.

Hobert, Guido:
Datenschutz und Datensicherheit im Internet, Interdependenz und Korrelation von rechtlichen Grundlagen und technischen Möglichkeiten, Frankfurt am Main, u.a. 1998

Hochstein, Reiner:
Teledienste, Mediendienste und Rundfunkbegriff – Anmerkungen zur praktischen Abgrenzung multimedialer Erscheinungsformen, NJW 1997, S. 2977 ff.

Hoenike, Mark / Hülsdunk, Lutz:
Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwilligung?, MMR 2004, S. 788 ff.

Hoeren, Thomas:
Grundzüge des Internetrechts, 2. Auflage, München 2002

Hoeren, Thomas:
Vorschlag für eine EU-Richtlinie über E-Commerce, MMR 1999, S. 192 ff.

Hoeren, Thomas:
Wegerechte auf dem Prüfstand, MMR 1998, S. 1 ff

Hoeren, Thomas:
Auskunftspflichten der Internetprovider an Strafverfolgungs- und Sicherheitsbehörden – eine Einführung, wistra 2005, S. 1 ff.

Hohmeister, Frank / Küper, Anja:
Individualvertragliche Arbeitszeitregelung bei der alternierenden Telearbeit, NZA 1998, S. 1206 ff.

Holznagel, Bernd / Enaux, Christoph / Nienhaus, Christian:
Grundzüge des Telekommunikationsrechts, Rahmenbedingungen, Regulierungsfragen, Internationaler Vergleich, 2. Auflage, München 2001

Holznagel, Bernd / Enaux, Christoph / Nienhaus, Christian:
Telekommunikationsrecht, Rahmenbedingungen – Regulierungspraxis, 2. Auflage, München 2006

Holznagel, Bernd:
Domainnamen- und IP-Nummern-Vergabe – eine Aufgabe der Regulierungsbehörde?, MMR 2003, S. 219 ff.

Horns, Axel:
Datenschutz in Kanzleien und Dienststellen – technische Fallstricke und Lösungsmöglichkeiten, in: Abel, Ralf (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, München 2003

Hornung, Gerrit:
Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, S. 3 ff.

Imhof, Ralf:
One-to-One-Marketing im Internet – Das TDDSG als Marketinghinweis, CR 2000, S. 110 ff.

Intveen, Michael / Lohmann, Lutz:
Die Haftung des Providers bei ASP-Verträgen: ITRB 2002, S. 210 ff.

Jacob, Joachim:
Perspektiven des neuen Datenschutzrechts, DuD 2000, S. 5ff.

Jandt, Silke:
Das neue TMG- Nachbesserungsbedarf für den Datenschutz im Mehrpersonenverhältnis, MMR 2006, S. 652 ff.

Janssen, Dirk, Thorsten:
Die Regulierung abweichenden Verhaltens im Internet, Eine Untersuchung verschiedener Regulierungsansätze unter besonderer Berücksichtigung der deutschen Rechtsordnung, Baden-Baden 2003

Jarass, Hans D.:
Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, S. 857 ff.

Jeserich, Hans-Dieter:
TK-Überwachung in Zahlen und Fakten, in: Holznagel Bernd / Nelles, Ursula / Sokol, Bettina, Die neue TKÜV (Telekommunikationsüberwachungsverordnung), S. 63 ff., in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 27, München 2002

Joecks, Wolfgang / Miebach, Klaus:
Münchener Kommentar zum Strafgesetzbuch, Band 3, §§ 185-262 StGB, München 2003 (zitiert: Bearbeiter in: Münchener Kommentar zum Strafgesetzbuch)

Kaminski, Bert / Henßler, Thomas / Kolaschnik, Helge, F./ Anastasia Papathoma-Baetge:
Rechtshandbuch E-Business, Neuwied u.a. 2002 (zitiert: Bearbeiter in: Kaminski/Henßler/Kolaschnik/Papathoma-Baetge, Rechtshandbuch E-Business)

Kieper Marcus:
Datenschutz für Telearbeitnehmer, DuD 1998, S. 583 ff.

Kilian, Wolfgang:
Informationelle Selbstbestimmung und Marktprozesse, Zur Notwendigkeit der Modernisierung des Modernisierungsgutachtens zum Datenschutzrecht, CR 2002, S. 921 ff.

Kittner, Michael / Zwanziger, Bertram (Hrsg.):
Arbeitsrecht, Handbuch für die Praxis, 3. Auflage, Frankfurt am Main 2005 (zitiert: Bearbeiter in: Kittner/Zwanziger, Arbeitsrecht)

Klaes, Sike:
Aktuelle Entwicklungen des TK-Kundenschutzes in Deutschland und in der EU, MMR 2006, S. 641 ff.

Kleine-Voßbeck, Bernd:
Electronic Mail und Verfassungsrecht, Marburg 2000

Kloepfer, Martin:
Privatsphäre im Fadenkreuz staatlicher Überwachung?, in:
Holznagel Bernd / Nelles, Ursula / Sokol, Bettina, Die neue TKÜV (Telekommunikationsüberwachungsverordnung), S. 91 ff., in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 27, München 2002

Klöpfer, Michael /Neun, Andreas:
Informationsrecht, München 2002

Knothe, Matthias:
Neues Recht für Multi-Media-Dienste, Die Ländersicht, AfP 1997, S. 494 ff.

Koch, Frank, A.:
Internet-Recht, Praxishandbuch mit dem neuen Medien- und Teledienstrecht, Checklisten und Musterverträge, 2. Auflage, München 2005

Koch, Frank, A.:
Perspektiven für die Link- und Suchmaschinen-Haftung, Kommissionsbericht zur Umsetzung der E-Commerce-Richtlinie und seine Konsequenzen für das TDG, CR 2004, S. 213 ff.

Koch, Frank, A.:
Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen, CR 1997, S. 193 ff.

Köcher, Jan K. / Kaufmann, Noogie C.:
Speicherung von Verkehrsdaten bei Internet-Access-Providern, Anmerkung zum Urteil des LG Darmstadt, DuD 2006, S. 360 ff.

Koenig Christian / Lotz, Sascha:
Sperrungsanordnungen gegenüber Network- und Access-Providern, CR 1999, S. 438 ff.

Koenig, Christian / Kühling, Jürgen:
Reformansätze des deutschen Telekommunikationsrechts in rechtsvergleichender Perspektive, MMR 2001, S. 80 ff.

Koenig, Christian / Neumann, Andreas:
Internet-Protokoll-Adresse als „Nummern“ im Sinne des Telekommunikationsrechts?, K&R 1999, S. 145 ff.

Koenig, Christian / Neumann, Andreas:
Telekommunikationsrechtliche Regulierung von Domainnamen, CR 2003, S. 182 ff.

Koenig, Christian / Röder, Ernst:
Die EG-Datenschutzrichtlinie für Telekommunikation – Verpflichtungen auf für Internetdienstleister, CR 2000, S. 668 ff.

Köhler, Helmut / Piper, Henning:
Gesetz gegen den unlauteren Wettbewerb, mit Zugabeverordnung, Rabattgesetz und Preisangabenverordnung, 3. Auflage, München 2002

Köhler, Markus / Arndt, Hans-Wolfgang / Fetzer, Thomas:
Recht des Internet, 5. Auflage, Heidelberg 2006

Köhntopp, Marit / Köhntopp, Kristian:
Datenspuren im Internet, CR 2000, S. 248 ff.

Königshofen, Thomas:
Die Umsetzung von TKG und TDSV durch Netzbetreiber, Service-Provider und Telekommunikationsanbieter, RDV 1997, S. 97 ff.

Königshofen, Thomas / Ulmer, Claus-Dieter
Datenschutz-Handbuch Telekommunikation, 1. Auflage, Frechen 2006

Körner, Marita:
Telearbeit – neue Form der Erwerbsarbeit, alte Regeln?, NZA 1999, S. 1190 ff.

Krader, Gabriela:
Moderne Online-Kommunikationsdienstleistungen im Spannungsverhältnis zwischen TKG und TDG, in: Königshofen, Thomas (Hrsg.), Das neue Telekommunikationsrecht in der Praxis, S. 115 ff., Heidelberg 1999

Kramer, Stefan:
Internetnutzung als Kündigungsgrund, NZA 2004, 457 ff.

Kramer, Philipp / Herrmann, Michael:
Auftragsdatenverarbeitung, Zur Reichweite der Privilegierung durch den Tatbestand des § 11 Bundesdatenschutzgesetz, CR 2003, S. 938 ff.

Kröger, Detlef / Gimmy, Marc A.:
Handbuch zum Internetrecht, Electronic Commerce, Informations-, Kommunikations- und Mediendienste, 2. Auflage, Heidelberg u.a. 2002

Kröger, Detlef / Gimmy, Marc A.:
Handbuch zum Internetrecht, Electronic Commerce, Informations-, Kommunikations- und Mediendienste, 1. Auflage, Berlin u.a.2001

Kröger, Detlef / Göers, Jutta / Hanken, Claas:
Internet für Juristen, Weltweiter Zugriff auf juristische Informationen, 2. Auflage, Neuwied, u.a. 1998

Kröger, Detlef / Kuner, Christopher:
Internet für Juristen, 3. Auflage, München 2001

Kröger, Detlef / Moos, Flemming:
Mediendienst oder Teledienst?, AfP 1997, S. 675 ff.

Kröger, Detlef / Moos, Flemming:
Regelungsansätze für Multimediadienste – Mediendienstestaatsvertrag und Teledienstegesetz, ZUM 1997, S. 462 ff.

Kröger, Detlef:
Rechtsdatenbanken, Angebote, Inhalte, Kosten, Wissensmanagement, München 2001

Kroiß, Ludwig / Schuhbeck, Sebastian:
Jura online, Recherchieren im Internet und Datenbanken, Neuwied, u.a. 2000

Kube, Hanno / Schütze, Marc:
Die Kosten der TK-Überwachung, Zum Ausgleich einer staatlichen Inpflichtnahme, CR 2003, S. 663 ff.

Kubicek, Herbert:
Probleme des Datenschutzes bei der Kommunikationsverarbeitung im ISDN, CR 1990, S. 659 ff.

Kuch, Hansjörg:
Der Staatsvertrag über Mediendienste, ZUM 1997, S. 225 ff.

Kunz, Jürgen:
Betriebs- und Geschäftsgeheimnisse und Wettbewerbsverbot während der Dauer und nach Beendigung des Anstellungsverhältnisses, DB 1993, S. 2482 ff.

Lackner, Karl / Kühl, Kristian (Hrsg.):
Strafgesetzbuch, 25. Auflage, München 2004

Ladeur, Karl-Heinz:
Das europäische Telekommunikationsrecht im Jahr 2002, Zur Vollendung des „Telekommunikationspakets“ (2001) durch ergänzende Richtlinien und zu einer Empfehlung der Kommission zur Marktabgrenzung sowie zur Entscheidungspraxis der europäischen Gerichte und der EG-Kommission auf dem Gebiet des Telekommunikations- und des Wettbewerbsrechts, K&R 2003, S. 153 ff.

Ladeur, Karl-Heinz:
Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, S. 372 ff.

Lehnhardt, Joachim:
Löschung virenbehafteter Emails, DuD 2003, S. 487 ff.

Leopold, Nils:
Protokollierung und Mitarbeiterdatenschutz, DuD 2006, S. 274 ff.

Lewinski, Kai von:
Kaufleute im Schutzbereich des BDSG, DuD 2000, S. 39 ff.

Lewinski, Rüpke von:
Bundesdatenschutzgesetz, Kommentar zum Bundesdatenschutzgesetz, NJW 2004, S. 349 ff.

Lienemann, Gerhard:
Virtuelle Private Netzwerke, Aufbau und Nutzen, Berlin 2002

Linnenkohl, Karl / Schütz, Regina: Anmerkung zu: Bundesarbeitsgericht (Urteil vom 22. Oktober 1986 – 5 AR 660/85): Erhebung, Speicherung und Löschung von Arbeitnehmerdaten, RDV 1987, S. 129 ff.

Lipp, Manfred:
VPN – Virtuelle Private Netzwerke, München, u.a. 2001

Löw, Petra:
Datenschutz im Internet, Eine strukturelle Untersuchung auf der Basis der neuen deutschen Medienordnung, Tübingen 2000

Mangoldt v., Herrmann / Klein, Friedrich / Starck, Christian:
Kommentar zum Grundgesetz, Band 1: Präambel, Artikel 1 bis 19, 5. Auflage, München 2005 (zitiert: Bearbeiter in: v.Mangoldt/Klein/Starck, GG Kommentar)

Manssen, Gerrit (Hrsg.):
Telekommunikations- und Multimediarecht, ergänzbarer Kommentar zum Telekommunikationsgesetz, Mediendienste-Staatsvertrag, Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz einschließlich Gesetzes- und Verordnungstexten von europäischen Vorschriften,
17. Ergänzungslieferung Stand Oktober 2006, Berlin (zitiert: Bearbeiter in: Manssen, Kommentar Telekommunikations- und Multimediarecht)

Mecklenburg, Wilhelm:
Internetfreiheit, ZUM 1997, S. 525 ff.

Mehrings, Josef:
Internet-Verträge und internationales Vertragsrecht, CR 1998, S. 613 ff.

Mengel, Anja:
Kontrolle der Telefonkommunikation am Arbeitsplatz, Wege durch einen juristischen Irrgarten?, BB 2004, S. 1445 ff.

Mengel, Anja:
Kontrolle der E-mail- und Internetkommunikation am Arbeitsplatz, BB 2004, S. 2014 ff.

Menzel, Hans-Joachim:
Genomanalyse im Arbeitsverhältnis und Datenschutz, NJW 1989, S. 2041 ff.

Molkenbur, Josef:
Pflicht zur Geheimniswahrung nach Ende des Arbeitsverhältnisses?, BB 1990, S. 1196 ff.

Moll, Wilhelm:
Telefondatenerfassung und betriebliche Mitbestimmung, Zugleich ein Beitrag zur Ermessensausübung der Einigungsstelle im Rahmen des § 87 Abs. 1 Nr. 6 BetrVG, DB 1982, S. 1722 ff.

Moll, Wilhelm:
Betriebliche Mitbestimmung beim Einsatz computergestützter Bildschirmarbeitsplätze, ZIP 1982, S. 892 ff.

Moos, Flemming:
Dürfen Access-Provider IP-Nummern speichern?, Analyse und Kritik der T-Online-Entscheidung der hessischen Datenschutz-Aufsichtsbehörde, CR 2003, S. 385 ff.

Moritz, Hans-Werner / Dreier, Thomas (Hrsg.):
Rechts-Handbuch zum E-Commerce, 2. Auflage, Köln 2005 (zitiert: Bearbeiter in: Moritz, Rechts-Handbuch zum E-Commerce)

Moritz, Hans-Werner / Niebler Angelika:
Internet-Telefonie im Spannungsfeld zwischen Sprachtelefondienst und Lizenzpflicht, CR 1997, S. 697 ff.

Moritz, Hans-Werner:
Rechtsfragen der Datenübermittlung bei internationalen Online-Diensten, in:
Büllesbach, Alfred (Hrsg.), Datenverkehr ohne Datenschutz?, Köln 1999, S. 95 ff.

Müller, Andreas:
Datenschutz beim betrieblichen E-Mailing, RDV 1998, S. 205 ff.

Müthlein, Thomas / Heck, Jürgen:
Outsourcing und Datenschutz, 3. Auflage, Frechen2006

Müthlein, Thomas:
Abgrenzungsprobleme bei der Auftragsdatenverarbeitung, RDV 1993, S. 165 ff.

Nägele, Stefan:
Internet und E-Mail: Abwehrrechte des Arbeitnehmers und Betriebsrats gegen unberechtigte Kontrollmaßnahmen des Arbeitgebers, ArbRB 2002, S. 55 ff

Nägele, Stefan / Meyer, Lars:
Internet und E-Mail am Arbeitsplatz: Rechtliche Rahmenbedingungen der Nutzung und Kontrolle sowie der Reaktion auf Missbrauch, K&R 2004, S. 312 ff.

Naujoks, Anke:
Internet-Richtlinien: Nutzung am Arbeitsplatz, DuD 2002, S. 592 ff.

Niedermeier, Robert / Damm, Maximilian:
Application Service Providing und Datenschutz, RDV 2001, S. 213 ff.

Niedermeier, Robert / Schröcker, Stefan:
Die „Homogene Datenschutzzelle“, RDV 2001, S. 90 ff.

Noack, Ulrich / Spindler, Gerald:
Unternehmensrecht und Internet, in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreiche Information und Recht, Band 20, München 2001

Nogala, Detlef / Haverkamp, Rita:
Elektronische Bewachung, Stichworte zur punitiven Aufenthaltskontrolle von Personen, DuD 2000, S. 31ff.

Nuthmann, Thomas:
Inkrafttreten des neuen UWG, ITRB 2004, S. 193 ff.

Ory, Stephan:
http://www.medienpolizei.de?, AfP 1996, S. 105 ff.

Oetker, Hartmut:
Die Ausprägung der Grundrechte des Arbeitnehmers in der Arbeitsordnung der Bundesrepublik Deutschland, RdA 2004, S. 8 ff.

Ohlenburg, Anna:
Der neue Telekommunikationsdatenschutz – Eine Darstellung von Teil 7 Abschnitt 2 TKG, MMR 2004, S. 431 ff.

Ossberger, Karl-Friedrich:
Betriebliche Kontrollen, ihre Voraussetzungen und Grenzen, zugleich ein Beitrag zur Diskussion um den Schutz und die Entfaltung der Persönlichkeit im Arbeitsverhältnis. Erlangen u.a. 1981

Pankoke, Stefan, L.:
Von der Presse- zur Providerhaftung, Eine rechtspolitische und rechtsvergleichende Untersuchung zur Inhaltsverantwortlichkeit im Netz, in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreiche Information und Recht, Band 14, München 2000

Pelz, Christian:
Die strafrechtliche Verantwortlichkeit von Internet-Providern, ZUM 1998, S. 530 ff.

Pernice, Ina, Maria:
Die Telekommunikations-Überwachungsverordnung (TKÜV), DuD 2002, S. 207 ff.

Peter, Stephan:
Verfügbarkeitsvereinbarungen beim ASP-Vertrag, Beschreibung der Leistung oder mängelhaftungsbeschränkende Abrede ?, CR 2005, S. 404 ff.

Petri, Axel / Göckel, Andreas:
Vertragsstruktur der Internet-Backbone-Betreiber: Peering, CR 2002, S. 418 ff.

Petri, Axel / Göckel, Andreas:
Vertragsstruktur der Internet-Backbone-Betreiber: Backbone-Access, CR 2002, S. 329 ff.

Pfitzmann, Andreas:
Datenschutz durch Technik, in:
Bäumler, Helmut / Mutius, Albert von (Hrsg.), Datenschutzgesetze der dritten Generation“ – Texte und Materialien zur Modernisierung des Datenschutzrechts, Neuwied, u.a. 1999

Pichler, Rufus:
Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG, MMR 1998, S. 79 ff.

Pieroth, Bodo / Schlink Bernhard:
Grundrechte, 22. Auflage, Heidelberg 2006

Post-Ortmann, Karin:
Der Arbeitgeber als Anbieter von Telekommunikations- und Telediensten, RDV 1999, S. 102 ff.

Prinz, Thomas:
Europäische Rahmenvereinbarung über Telearbeit, NZA 2002, S. 1268 ff.

Raffler, Andrea / Hellich, Peter:
Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer-e-mails zulässig ? NZA 1997, S. 862 ff

Rasmussen, Heike:
Datenschutz im Internet, CR 2002, S. 36 ff.

Räther, Philipp C. / Seitz, Nicolai:
Übermittlung personenbezogener Daten in Drittstaaten – Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, S. 425 ff.

Räther, Philipp C. / Seitz, Nicolai:
Ausnahmen bei Datentransfer in Drittstaaten – Die beiden Ausnahmen nach § 4c Abs. 2 BDSG: Vertragslösung und Code of Conduct, MMR 2002, S. 520 ff.

Räther, Philipp C.:
Datenschutz und Outsourcing, DuD 2005, S, 461 ff.

Rebmann, Kurt / Säcker, Franz, Jürgen (Hrsg.):
Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2, Schuldrecht, Allgemeiner Teil (§§ 241-432, FernAbsG), 4. Auflage München 2001 (zitiert: Bearbeiter in: Münchener Kommentar zum Bürgerlichen Gesetzbuch)

Rebmann, Kurt / Säcker, Franz, Jürgen (Hrsg.):
Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2a, Schuldrecht, Allgemeiner Teil (§§ 241-432), 4. Auflage, München 2003 (zitiert: Bearbeiter in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2a)

Reinermann, Heinrich (Hrsg.):
Datenschutz im Internet – Internet im Datenschutz, Speyer 2003

Richardi, Reinhard / Wlotzke, Otfried (Hrsg.):
Münchener Handbuch zum Arbeitsrecht, Band 3 (Kollektives Arbeitsrecht), 2. Auflage, München 2000 (zitiert: Bearbeiter in: Münchener Handbuch Arbeitsrecht)

Richter, Peter, C.:
Datenschutzrechtliche Aspekte beim Tele- und Homebanking, Frankfurt am Main, u.a. 1998

Riehmer, Klaus / Hessler, Christina:
Rahmenbedingungen und Ausgestaltung von Provider-Verträgen, CR 2000, S. 170 ff.

Rieß, Joachim:
Anwendbarkeit des TKG und des IuKDG auf Telekommunikationsdiensteanbieter, Service Provider und Telediensteanbieter, in: Bartsch, Michael / Lutterbeck, Bernd (Hrsg.), Neues Recht für neue Medien, S. 277 ff., Köln 1998

Rieß, Joachim:
Der Telekommunikationsdatenschutz bleibt eine Baustelle, DuD 1996, S. 328 ff.

Ritz, Dorothee:
Inhalteverantwortlichkeit von Online-Diensten: Strafbarkeit von Online-Diensten in ihrer Funktion als Inhalteanbieter, Online-Service-Provider und Internet-Access-Provider für die Verbreitung von Pornographie im elektronischen Datennetz, (Ein Rechtsvergleich), Frankfurt am Main, u.a. 1998

Röhrborn, Jens / Katko, Peter:
Rechtliche Anforderung an Wireless LAN, Eine Untersuchung nach deutschem und europäischem Kommunikationsrecht, CR 2002, S. 882 ff.

Röhrborn, Jens / Sinnhart, Michael:
Application Service Providing – juristische Einordnung und Vertragsgestaltung, CR 2001, S. 69 ff.

Rosen, Jeffrey:
The Unwanted Gaze, The Destruction of Privacy in America, New York, u.a. 2001

Rosenfelder, Ulrich:
Lexikon des Betriebsverfassungsrechts, Alphabetischer Leitfaden für die Praxis, Berlin 1992

Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen:
Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministerium des Innern (Hrsg.), Berlin 2001 (zitiert: Modernisierungsgutachten)

Roßnagel, Alexander/ Scholz, Philipp:
Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, S. 721 ff.

Roßnagel, Alexander (Hrsg.):
Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003 (zitiert: Bearbeiter in: Roßnagel, Handbuch Datenschutzrecht)

Roßnagel, Alexander:
Neues Recht für Multimediadienste, NVwZ 1998, S. 1 ff.

Roßnagel, Alexander (Hrsg.):
Recht der Multimedia-Dienste, Kommentar zum IuKDG und zum MDStV,
7. Ergänzungslieferung – Stand: 04/2005 (zitiert: Bearbeiter in: Roßnagel, Recht der Multimedia-Dienste)

Roßnagel, Alexander:
Vorwort, in: Roßnagel, Alexander (Hrsg.), Datenschutz beim Online-Einkauf, Braunschweig/Wiesbaden 2002

Roth, Birgit / Haber, Marc:
VPN-Verträge, Virtual Private Networks: technische Beschaffenheit, vertragstypologische Einordnung, vertraglicher Regelungsbedarf, ITRB 2004, S. 19 ff.

Rottenburg, Franz:
Rechtsprobleme beim Direktbanking, WM 1997, S. 2381 ff.

Ruppmann, Evelyn:
Der konzerninterne Austausch personenbezogener Daten, Baden-Baden 2000

Säcker, Franz Jürgen:
Berliner Kommentar zum Telekommunikationsgesetz, Schriftenreihe Kommunikation und Recht, Band 21, Frankfurt am Main 2006 (zitiert: Bearbeiter in: Berliner Kommentar zum TKG)

Sankol, Barry:
Die Qual der Wahl: § 113 TKG oder §§ 100g, h StPO? Die Kontroverse über das Auskunftsverlangen gegen Access-Provider bei dynamischen IP-Adressen, MMR 2006, S. 361 ff.

Schaar, Peter:
Datenschutz im Internet, Die Grundlagen, München 2002

Schaar, Peter:
Datenschutzfreier Raum Internet?, CR 1996, S. 170 ff.

Schaar, Peter:
Datenschutzrechtliche Einwilligung im Internet, MMR 2001, S. 644 ff.

Schäfer, Detmar:
ENUM - Domainnamensystem und Rufnummernraum wachsen zusammen, CR 2002, S. 690 ff.

Schaffland, Hans-Jürgen / Wiltfang, Noeme (Hrsg.):
Bundesdatenschutzgesetz (BDGS), Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Lieferung 2/06, Mai 2006, Berlin

Schaub, Günther, / Koch, Ulrich / Linck, Rüdiger (Hrsg.):
Arbeitsrechtshandbuch, Systematisch Darstellung und Nachschlagewerk für die Praxis, 11. Auflage, München 2005

Scheurle, Klaus-Dieter / Mayen, Thomas (Hrsg):
Telekommunikationsgesetz (TKG), München 2002

Schladebach, Marcus:
Genetische Daten im Datenschutzrecht, Die Einordnung genetischer Daten in das Bundesdatenschutzgesetz, CR 2003, S. 225 ff.

Schmidl, Michael:
Private E-Mail-Nutzung - Der Fluch der guten Tat, DuD 2005, S. 267 ff.

Schmitz, Florian:
Anmerkung zu LG Potsdam (Urteil vom 8. Juli 1999 – 3O 317/99): Zugangsvermittlung zu Meinungsmarkt, CR 2000, S. 123 ff.

Schmitz, Peter:
TDDSG und das Recht auf informationelle Selbstbestimmung, in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreiche Information und Recht, Band 12, München 2000

Schneider, Annette:
Verträge über Internet-Access, Typisierung der Basisverträge mit nicht-kommerziellen Anwendern, in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreiche Information und Recht, Band 22, München 2001

Schneider, Gerhard:
Die Wirksamkeit der Sperrung von Internet-Zugriffen, MMR 1999, S. 571 ff.

Schneider, Hans-Jochen:
Lexikon Informatik und Datenverarbeitung, 4. Auflage, München 1997

Schneider, Jochen:
Handbuch des EDV-Rechts, IT-Vertragsrecht – Rechtsprechung – AGB – Vertragsgestaltung – Datenschutz, Rechtsschutz, 3. Auflage, Köln 2003

Schoen, Thomas:
Rechtliche Rahmenbedingungen zur Analyse von Log-Files, DuD 2005, S. 84 ff.

Scholz, Philipp:
Datenschutzrechtliche Anforderungen, in:
Roßnagel, Alexander (Hrsg.), Datenschutz beim Online-Einkauf, Braunschweig/Wiesbaden 2002

Schönke, Adolf / Schröder, Horst:
Strafgesetzbuch, Kommentar, 27. Auflage, München 2006 (zitiert: Bearbeiter in: Schönke/Schröder, StGB)

Schrey, Joachim / Meister Matthias:
Beschränkte Verwendbarkeit von Standortdaten – Hemmschuh für den E-Commerce ?, K&R 2002, S. 177 ff.

Schulin, Bertram / Babl, Monika:
Rechtsfragen der Telefondatenverarbeitung, NZA 1986, S. 46 ff.

Schulz, Wolfgang:
Jenseits der „Meinungsrelevanz“ – Verfassungsrechtliche Überlegungen zu Ausgestaltung und Gesetzgebungskompetenzen bei neuen Kommunikationsformen, ZUM 1996, S. 487 ff.

Schulz, Wolfgang:
Verfassungsrechtlicher „Datenschutzauftrag“ in der Informationsgesellschaft, Schutzkonzepte zur Umsetzung informationeller Selbstbestimmung am Beispiel von Online-Kommunikation, Die Verwaltung 1999, S. 137 ff.

Schumacher, Volker A.:
Die Gestaltung von IP-VPN-Verträgen, Fragestellungen bei Verträgen über eine neue Form des Unternehmensnetzwerkes, CR 2006, S. 229 ff.

Schuppert, Stefan:
Web-Hosting-Verträge, CR 2000, S. 227 ff.

Schuster, Fabian / Müller, Ulf:
Entwicklung des Internet- und Multimediarechts von Januar 1999 bis Juni 2000, MMR-Beilage 10/2000, S. 1 ff.

Schütz, Raimund / Attendorn, Thorsten:
Anmerkung zu LG Frankenthal (Urteil vom 28. November 2000 -6 O 293/00): “Pfaelzer-Links“, MMR 2001, S. 401 ff.

Schütz, Raimund:
Telefondienst und Telekom-Monopol, Betriebs-Berater (BB) 1996, S. 1445 ff.

Schwarz, Mathias:
Arbeitnehmerüberwachung und Mitbestimmung, Das Mitbestimmungsrecht des Betriebsrats bei Einführung und Anwendung technischer Einrichtungen der Leistungs- und Verhaltenskontrolle, München u.a. 1982

Sieber, Ulrich / Hoeren, Thomas (Hrsg.):
Handbuch Multimedia-Recht, 16. Ergänzungslieferung – Stand 08/2006, München (zitiert Bearbeiter in: Hoeren/Sieber)

Sieber, Ulrich:
AG München: “Compuserve”-Urteil, MMR 1998, S. 429 ff.

Sieber, Ulrich:
Die rechtliche Verantwortlichkeit im Internet, MMR-Beilage 2/1999, S. 1 ff.

Sieber, Ulrich:
Die Verantwortlichkeit von Internet-Providern im Rechtsvergleich, ZUM 1999, S. 196 ff.

Simitis, Spiros / Dammann, Ulrich (Hrsg.):
EG-Datenschutzrichtlinie: Kommentare, Baden-Baden 1997

Simitis, Spiros:
Datenschutz – Rückschritt oder Neubeginn?, NJW 1998, S. 2473 ff.

Simitis, Spiros (Hrsg.):
Kommentar zum Bundesdatenschutzgesetz, 5. Auflage, Baden-Baden 2006 (zitiert: Bearbeiter in: Simitis, BDSG-Kommentar)

Simon, Joachim:
Die Verleihungsverordnung nach §2 Absatz 2 des Gesetzes über Fernmeldeanlagen, Archiv Telekommunikation 1996, S. 142 ff.

Söbbing, Thomas:
Vertragsgestaltung und Vertrags-Management zur Sicherung der Kundenzufriedenheit bei IT-Sourcing und BPO-Projekten in: *Köhler-Frost, Wilfried (Hrsg.),* Outsourcing, Schlüsselfaktoren der Kundenzufriedenheit, 5. Auflage, Berlin 2005

Sonntag, Matthias:
IT-Sicherheit kritischer Infrastrukturen, Von der Staatsaufgabe zur rechtlichen Ausgestaltung, in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 48, München 2005

Spindler, Gerald (Hrsg.):
Vertragsrecht der Internet-Provider, Köln 2000 (zitiert: Bearbeiter in: Spindler, Vertragsrecht der Internet-Provider (1. Auflage))

Spindler, Gerald (Hrsg.):
Vertragsrecht der Internet-Provider, 2. Auflage, Köln 2005 (zitiert: Bearbeiter in: Spindler, Vertragsrecht der Internet-Provider (2. Auflage))

Spindler, Gerald (Hrsg.):
Vertragsrecht der Telekommunikationsanbieter, Köln 2000

Spindler, Gerald / Volkmann, Christian:
Die öffentlich-rechtliche Störerhaftung der Access-Provider, K&R 2002, S. 398 ff.

Spindler, Gerald:
Neues im Vertragsrecht der Internet-Provider, Einflüsse der Reformen des Schuldrechts und des Telekommunikationsrechts, CR 2004, S. 203 ff.

Spindler, Gerald:
Anmerkung zu BGH (Urteil vom 23. September 2003 – VI ZR 335/02): Haftung des Internetproviders für fremde Inhalte, CR 2004, S. 48 ff.

Spindler, Gerald:
Der neue Vorschlag einer E-Commerce-Richtlinie, ZUM 1999, S. 775 ff.

Spindler, Gerald:
Dogmatische Strukturen der Verantwortlichkeit der Diensteanbieter nach TDG und MDStV, MMR 1998, S. 639 ff.

Spindler, Gerald:
E-Commerce in Europa, Die E-Commerce-Richtlinie in ihrer endgültigen Fassung, MMR 2000, S. 4 ff.

Spindler, Gerald:
E-Commerce in Europa, MMR-Beilage 7/2000, S. 4 ff.

Spindler, Gerald:
Haftungsrechtliche Grundprobleme der neuen Medien, NJW 1997, S. 3193 ff.

Spindler, Gerald:
Zugangsgewährung durch Internet-Provider – Typische Klauseln und Inhaltskontrolle, K&R 1999, S. 488 ff.

Spindler, Gerald:
Die Verantwortlichkeit der Provider für “Sich-zu-eigen-gemachte” Inhalte und für beaufsichtigte Nutzer, MMR 2004, S. 440 ff.

Spindler, Gerald / Schmitz, Peter / Geis, Ivo:
TDG, Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz, Kommentar, München 2004 (zitiert: Bearbeiter in: Spindler/Schmitz/Geis)

Spindler, Gerald / Dorschel, Joachim:
Vereinbarkeit der geplanten Auskunftsansprüche gegen Internet-Provider mit EU-Recht, CR 2006, S. 341 ff.

Spindler, Gerald / Börner, Fritjof (Hrsg):
E-Commerce-Recht in Europa und den USA, Berlin u.a. 2003

Sponeck, Henning von:
Überlassung von RZ-Kapazität – ein Fall der Auftragsdatenverarbeitung?, CR 1992, S. 594 ff.

Sprenger, Wolfgang / Fischer, Thomas:
Zur Erforderlichkeit der richterlichen Anordnung von DNA-Analysen; NJW 1999, S. 1830 ff.

Stadler, Thomas:
Sperrungsverfügung gegen Access-Provider, MMR 2002, S. 343 ff.

Statz, Klaus-Peter:
Zehn Jahre privatrechtliche Kundenbeziehung in der Telekommunikation, in: Königshofen, Thomas (Hrsg.), Das neue Telekommunikationsrecht in der Praxis, Heidelberg 1999, S. 65 ff.

Steckler, Brunhilde:
Grundzüge des IT-Rechts, 2. Auflage, München 2006

Steding, Ralf:
Outsourcing von Bankdienstleistungen: Bank- und datenschutzrechtliche Probleme der Aufgabenverlagerung von Kreditinstituten auf Tochtergesellschaften und sonstige Dritte; BB 2001, S. 1693 ff.

Stransfeld, Reinhard:
Regelungen in der Informationstechnik und Telekommunikation – Informationshemmnisse durch Recht?, in: Schulte Martin (Hrsg.), Technische Innovation und Recht, Antrieb oder Hemmnis, S. 167 ff. Heidelberg 1996

Strömer, Tobias, H.:
Online-Recht, Rechtsfragen im Internet, 4. Auflage, Heidelberg 2006

Struck, Volker;
Hinweis auf die Rechtsfolgen der Löschung von Verbindungsdaten – Vorvertragliche Pflichten von TK-Diensteanbietern infolge überlegener Sach-/Rechtskunde?, MMR 2001, S. 507 ff.

Summa, Harald, A.:
Was sagen die Internetprovider, in: Holznagel Bernd / Nelles, Ursula / Sokol, Bettina, Die neue TKÜV (Telekommunikationsüberwachungsverordnung), S. 24 ff., in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 27, München 2002

Taeger, Jürgen:
Verschwiegenheitspflicht im Arbeitsrecht, Arbeit und Arbeitsrecht 1992, S. 201 ff.

Tanenbaum, Andrew, S.:
Computernetzwerke, 4. Auflage, München u.a. 2003

Tanenbaum, Andrew, S.:
Computerarchitektur, Strukturen – Konzepte – Grundlagen, 5. Auflage, München u.a. 2006

Teia (Hrsg.):
Recht im Internet, Berlin 2002

De Terwagne, Cecile / Louveaux, Sophie:
Data Protection and Online Networks, MMR 1998, S. 451 ff.

Tettenborn, Alexander:
Die Evaluierung des IuKDG, Erfahrungen, Erkenntnisse und Schlußfolgerungen:
MMR 1999, S. 516 ff.

Tiedemann, Jens:
Speicherung von Verbindungsdaten zu 0190-Rufnummern, ITRB 2003, S. 217 ff.

Tinnefeld, Marie-Theres:
Die Novellierung des BDSG im Zeichen des Gemeinschaftsrechts, NJW 2001, S. 3078 ff.

Tinnefeld, Marie-Theres:
Aktuelle Fragen des Arbeitnehmerdatenschutzes, DuD 2002, S. 231 ff.

Tinnefeld, Marie-Theres:
Arbeitnehmerdatenschutz in Zeiten des Internet, MMR 2001, S. 797 ff.

Tinnefeld, Marie-Theres / Ehmann, Eugen / Gerling, Rainer, W.:
Einführung in das Datenschutzrecht, 4. Auflage, München 2005

Tinnefeld, Marie-Theres / Ehmann, Eugen:
Einführung in das Datenschutzrecht, 3. Auflage, München 1998

Tinnefeld, Marie-Therese / Viethen, Hans Peter:
Arbeitnehmerdatenschutz und Internet-Ökonomie – Zu einem Gesetz über Information und Kommunikation im Arbeitsverhältnis, NZA 2000, S. 977 ff.

Tröndle, Herbert / Fischer, Thomas:
Strafgesetzbuch und Nebengesetze, Beck'sche Kurzkommentare, Band 10, 53. Auflage München 2006

Trute, Hans-Heinrich / Spörr, Wolfgang / Bosch, Wolfgang:
Telekommunikationsgesetz mit FTEG, Berlin, u.a. 2001

Ueckert, André:
Private Internet- und E-Mail-Nutzung am Arbeitsplatz, Entwurf einer Betriebsvereinbarung, ITRB 2003, S. 158 ff.

Ullrich, Jürgen:
Was meinen die Macher, in:
Holznagel Bernd / Nelles, Ursula / Sokol, Bettina, Die neue TKÜV (Telekommunikationsüberwachungsverordnung), S. 15 ff., in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 27, München 2002

Ulmer, Claus, D.:
IT-Outsourcing und Datenschutz bei der Erfüllung öffentlicher Aufgaben, CR 2003, S. 701 ff.

Ulmer, Peter / Brandner, Hans, Erich / Hensen, Horst-Diether / Schmidt, Harry:
AGB-Gesetz, Kommentar zum Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen, 9. Auflage, Köln 2001 (zitiert: Bearbeiter in: Ulmer/Brandner/Hensen)

Vassilaki, Irini, E.:
OVG Nordrhein-Westfalen: Sperrverfügung gegen Access-Provider rechtmäßig, CR 2003, S. 367 ff.

Vassilaki, Irini, E.:
Strafrechtliche Verantwortlichkeit der Diensteanbieter nach dem TDG, MMR 1998, S. 630 ff.

Volkmann, Christian:
Anmerkung zu VG Düsseldorf „Sperrungsverfügung gegen Access-Provider, CR 2005, S. 885 ff.

Voss, Andreas:
Das große PC & Internet Lexikon 2007, Düsseldorf 2006

Voss, Andreas:
Das große PC & Internet Lexikon 2004, Düsseldorf 2004

Voßbein, Reinhard:
IT-Outsourcing – ein Beitrag zum Lean-Management?, RDV 1993, S. 205 ff.

Wächter, Michael:
Rechtliche Grundstrukturen der Datenverarbeitung im Auftrag, CR 1991, S. 333 ff.

Waldenberger, Arthur:
Der juristische Dauerbrenner: Haftung für Hyperlinks im Internet – ein Fall des LG Hamburg, AfP 1998, S. 373 ff.

Waldenberger, Arthur:
Teledienste, Mediendienste und die „Verantwortlichkeit“ ihrer Anbieter, MMR 1998, S. 124 ff.

Wanckel, Endress:
Persönlichkeitsschutz in der Informationsgesellschaft, Zugleich ein Beitrag zum Entwicklungsstand des allgemeinen Persönlichkeitsrechts, in: Europäische Hochschulschriften, Frankfurt am Main, u.a. 1999

Wank, Rolf:
Telearbeit, NZA 1999, S. 225 ff.

Wedde, Peter / Noll, Gerhard:
Gesetzestexte für die Arbeitswelt, 2. Auflage, Düsseldorf/Hamburg 2005

Wedde, Peter:
Aktuelle Rechtsfragen der Telearbeit, NJW, 1999, S. 527 ff.

Wedde, Peter:
Datenschutz bei Telearbeit, DuD 1998, S. 576 ff.

Wedde, Peter:
Digitalisierung der Arbeitswelt und Telearbeit – keine Chance für das Arbeitsrecht ?, RDV 1996, S. 5 ff.

Wedde, Peter:
Telearbeit und Mitbestimmung des Betriebsrats, CR 1994, S. 230 ff.

Wedde, Peter:
Die wirksame Einwilligung im Arbeitnehmerdatenschutzrecht, DuD 2004, S. 169 ff.

Wedde, Peter:
Schutz vor verdeckten Kontrollen im Arbeitsverhältnis, DuD 2004, S. 21 ff.

Wedde, Peter:
Telearbeit, Arbeitsrecht-Sozialrecht-Datenschutz, München 2002

Wedde, Peter:
Anmerkung zu BAG vom 27.03.2003 (2 AZR 51/02), BAG vom 29.06.2004 (1 ABR 21/03) sowie BAG vom 14.12.2004 (1 ABR 34/03), AuR 2005, S. 453 ff.

Wedde, Peter / Klöver, Karen:
Outsourcing. Das Ende der Mitbestimmung ?, CR 1993, S. 93 ff.

Wegel, Wolfgang:
Presse und Rundfunk im Datenschutz : zur Regelung des journalistischen Umgangs mit personenbezogenen Daten, Frankfurt am Main, u.a. 1994

Weichert, Thilo:
Der Entwurf eines Bundesdatenschutzgesetzes von Bündnis90/Die Grünen, in: Bäumler, Helmut / Mutius, Albert von (Hrsg.), Datenschutzgesetze der dritten Generation“ – Texte und Materialien zur Modernisierung des Datenschutzrechts, Neuwied, u.a. 1999

Weichert, Thilo:
Der Entwurf eines Bundesdatenschutzgesetzes von Bündnis 90/Die Grünen, RDV 1999, S. 65 ff.

Weichert, Thilo:
Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, S. 1463 ff.

Weiler, Frank:
Spamming – Wandel des europäischen Rechtsrahmens, MMR 2003, S. 223 ff.

Weißnicht, Elmar:
Die Nutzung des Internet am Arbeitsplatz, MMR 2003, S. 448 ff.

Welp, Jürgen:
Die TKÜV im System staatlicher Abhörbefugnisse, in:
Holznagel Bernd / Nelles, Ursula / Sokol, Bettina, Die neue TKÜV (Telekommunikationsüberwachungsverordnung), S. 3 ff., in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 27, München 2002

Wenzel, Jörg:
Europa und die neuen Informations- und Telekommunikationstechnologien, RDV 1996, S. 10 ff.

Wesser, Sabine:
Der Schutz der räumlichen Privatsphäre bei Wohnungsdurchsuchungen nach §§ 758, 758a ZPO, NJW 2002, S. 2138 ff.

Westerholt, Margot, Gräfin von /Berger, Konrad:
Der Application Service Provider und das neue Schuldrecht, Vertragsrechtliche Fragen zu seiner Stellung zwischen Lieferanten und Kunden, CR 2002, S. 81 ff.

Westphalen, Friedrich, Graf von:
Ausgewählte arbeits- und datenschutzrechtliche Fragen beim „Outsourcing“ um Rahmen von § 25a Abs. 2 KWG, WM 1999, S. 1810 ff.

Wiebe, Andreas:
Know-how-Schutz von Computersoftware, 1. Auflage, München 1993

Wiese, Günther:
Anmerkung zu BAG AP Nr. 40 zu § 87 BetrVG 1972 „Überwachung“

Wiese, Günther:
Das Initiativrecht nach dem Betriebsverfassungsgesetz, Neuwied u.a. 1977

Wiese, Günther:
Genetische Analyse bei Arbeitnehmern, RdA 1986, S. 120 ff.

Wildemann, Daniela:
Vertragsschluß im Netz, in: Lehmann, Michael, Rechtswissenschaftliche Forschung und Entwicklung (Hrsg.), Band 642, München 2000

Wimmer, Norbert / Michael, Gerhard:
Der Online-Provider im neuen Multimediarecht, Baden-Baden 1998

Wimmer, Norbert:
Die Verantwortlichkeit des Online-Providers nach dem neuen Multimediarecht – zugleich ein Überblick über die Entwicklung der Rechtssprechung seit dem 1.8.1997, ZUM 1999, S. 436 ff.

Wischmann, Tim:
Rechtsnatur des Access-Providing, MMR 2000, S. 461 ff.

Wlotzke, Otfried / Preis, Ulrich:
Betriebsverfassungsgesetz, Kommentar, 3. Auflage, München 2006 (zitiert: Bearbeiter in: Wlotzke/Preis, BetrVG)

Wronka, Georg:
Zur Interessenlage bei der Auftragsdatenverabeitung, RDV 2003, S. 132 ff.

Wuermeling, Ulrich / Felixberger, Stefan:
Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz, CR 1997, S. 230 ff.

Wuermeling, Ulrich:
Scoring von Kreditrisiken, NJW 2002, S. 3508 ff.

Wulf, Hans, Markus:
Serververträge und Haftung für Serverausfälle, Eine Analyse der vertragstypologischen Einordnung und des Haftungsumfangs, CR 2004, S. 43 ff.

Wülfing, Thomas:
Keine Sachbeschädigung durch unerwünschte Telefaxwerbung, ITRB 2004, S. 152 ff.

Zilkens, Martin / Werhahn, Ruth:
Datenschutz und Datensicherheit bei Telearbeit in der Kommunalverwaltung, RDV 1999, S. 60 ff.

Zilkens, Martin:
Datenschutz am Arbeitsplatz, DuD 2005, S. 253 ff.

Zimmer, Anja:
Wireless LAN und das Telekommunikationsrecht, Verpflichtungen für Betreiber nach bisherigem und künftigem Recht, CR 2003, S. 893 ff.

Zimmermann, Andreas:
Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, S. 3145 ff.

Zwingel, Wolfgang:
Technische Überwachungsmaßnahmen aus Sicht der Polizei, in: Holznagel Bernd / Nelles, Ursula / Sokol, Bettina, Die neue TKÜV (Telekommunikationsüberwachungsverordnung), S. 37 ff., in: Hoeren, Thomas / Spindler, Gerald / Holznagel, Bernd / Gounalakis, Georgios / Burkert, Herbert (Hrsg.), Schriftenreihe Information und Recht, Band 27, München 2002

Sonstige Materialien

A. Websites

Hinweis: Im folgenden werden lediglich Internetseiten mit rechtlichem Bezug aufgelistet, so dass insbesondere auf die Angabe der URL-Adressen von Produktbeschreibungen verzichtet wird. Die entsprechenden Nachweise sind jedoch in den jeweils relevanten Fußnoten zu finden.

1. Entwurf des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz- EIGVG) vom 19.04.2005, abrufbar unter http://www.computerundrecht.de/docs/entwurf_eigvg_19_4_2005.pdf (Website vom 30.09.2006)

2. Gesetzentwurf des Telekommunikationsgesetzes (TKG) vom 15.10.2003, abrufbar unter http://www.computerundrecht.de/docs/tkg_e_entwurf_mit_begruendungpropertypdf.pdf (Website vom 30.09.2006), zitiert als TKG-E

3. Vorschlag für ein Gesetz über den Datenschutz bei der Nutzung elektronischer Medien (EMDSG), abrufbar unter http://www.dud.de/dud/documents/emediendatsch030402.pdf (Website vom 30.09.2006)

4. Begründung zum Entwurf einer Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV) des Bundesbeauftragten für den Datenschutz, abrufbar unter www.bfd.bund.de/information/symp2_ulrich3.html (Website vom 01.08.2004)

5. IT-Grundschutz-Kataloge, Sicherheit in der Informationstechnik, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik, Loseblattsammlung, Stand 2005, www.bsi.de bzw. http://www.bsi.de/gshb/deutsch/index.htm (Website vom 30.09.2006)

6. Informationen und Ausführungen der Bundesnetzagentur zur Technischen Umsetzung von Überwachungsmaßnahmen, abrufbar unter http://www.bundesnetzagentur.de/enid/78f203c9cbedb13a969685e262e885f3,55a304092d09/Technische_Regulierung_Telekommunikation/Technische_Umsetzung_von_Ueberwachungsma_nahmen_h6.html
   sowie
   http://www.bundesnetzagentur.de/enid/78f203c9cbedb13a969685e262e885f3,55a304092d09/Technische_Umsetzung_von_Ueberwachungsma_nahmen/Zusaetzliche_Informationen_fuer_die_Betreiber_von_E-_np.html
   (Websites vom 30.09.2006)

B. Fundstellen in gesonderter Form

I. Datenschutz-/Tätigkeitsberichte

1. 14. Datenschutzbericht der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen, Düsseldorf 1999

2. 32. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Wiesbaden 2003

3. *Bundesbeauftragter für den Datenschutz (Hrsg.):*
   Datenschutz in der Telekommunikation, BfD Info5, 5. Auflage, Bonn 2001

II. Europäische Kommission

1. Mitteilung der europäischen Kommission, KOM (87) 290 endg., „Auf dem Wege zu einer dynamischen europäischen Volkswirtschaft", Grünbuch über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte, Brüssel, 30. Juni 1987

2. Vorschlag der Kommission der europäischen Gemeinschaften für eine Richtlinie des europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt vom 18.11.1998 KOM (1998) 586 endg. (zitiert: „Vorschlag der Kommission")

III. Zeitungsartikel

1. *Frankfurter Allgemeine Zeitung vom 19. Januar 2002, S. 19*
   Unternehmen brauchen Schutz gegen IT-Risiken
   Versicherungen häufig unzureichend / Haftungsgefahr für die Geschäftsführung

2. *Frankfurter Allgemeine Zeitung vom 21. Januar 2002, S. 23*
   Jedes zweite Großunternehmen wird von Computerhackern über das Internet angegriffen
   Professionelle Hacker-Szene / Banken, Versicherungen und Technologieunternehmen sind beliebte Ziele für Wirtschaftsspionage und Erpressung

3. *Frankfurter Allgemeine Zeitung vom 21. März 2002, S. 21*
   Sicherheit ist das wichtigste IT-Thema in diesem Jahr
   Schäden in Millionenhöhe / Mitarbeiter genauer beobachten / "Intrusion Detection" auf dem Vormarsch

4. *Frankfurter Allgemeine Zeitung vom 11. April 2002, S. 22*
   Zahl der Attacken auf Computersysteme erreicht Höchststand
   Immer mehr Angriffe aus dem Internet / Viren verursachen hohe Schäden / Hybride Angriffe nehmen zu / Biometrie bleibt Nischenthema

5. *Frankfurter Allgemeine Zeitung vom 27. Januar 2003, S. 22*
   Intelligente Hacker kommen an der Firewall vorbei in das Unternehmen
   Computerangriffe aus dem Internet nehmen zu / Kommunikation mit Kunden und Partnern öffnet Eindringlingen die Tür in das Firmennetz

6. *Frankfurter Allgemeine Zeitung vom 10. Februar 2003, S. 15*
   Hacker finden immer mehr Schwachstellen in den Schutzmauern der Firmennetze
   Angriffe kommen aus Amerika und Südkorea / Energiekonzerne sind beliebte Ziele / Internet Explorer als Risikofaktor / Kein Cyber- Terrorismus

7. *Frankfurter Allgemeine Zeitung vom 23. Februar 2004, S. 17*
   Wimax-Technik bedroht DSL-Geschäft (Langfristig auch Konkurrenz zu UMTS)

8. *Frankfurter Allgemeine Zeitung vom 14. März 2003, S. 24*
   Telekom bringt das Internet auf das Fernsehen
   Notwendige Set-Top-Box soll mindestens 800 Euro kosten / Filme kommen per DSL oder Satellit

9. *Frankfurter Allgemeine Zeitung vom 18. Juni 2004, S.12*
   Service-Rufnummern künftig aus allen Netzen erreichbar (Deutsche Telekom einigt sich mit Wettbewerbern über Abrechnung von Mehrwertdiensten)

10. *Frankfurter Allgemeine Zeitung vom 23. August 2004, S. 17*
    Der „Bankraub per E-Mail“ kommt in Mode (Kunden von Ebay, der Deutschen Bank und Postbank im Visier von Internet-Betrügern / „Phishing“ in Deutschland

Neue Online-Dienste und Datenschutz
am Beispiel von Virtuellen Privaten Netzwerken

1. Teil Einführung

A. Bedeutung des Themas

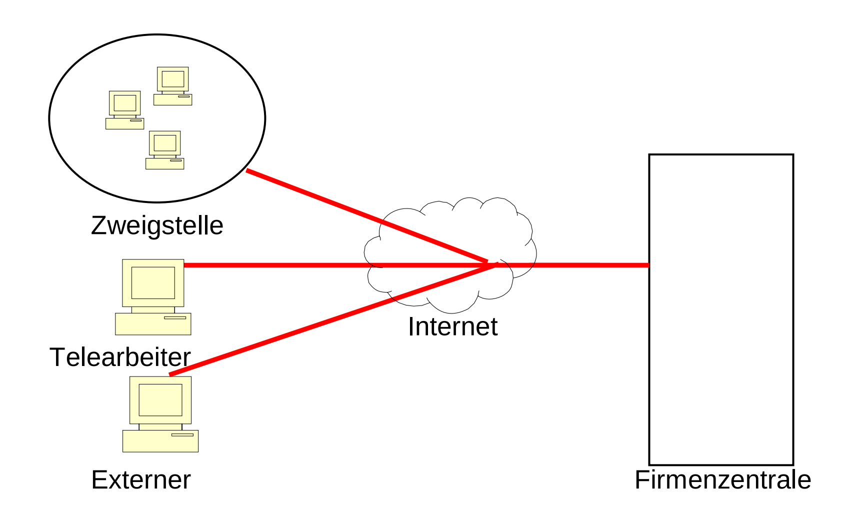
In der jüngeren Vergangenheit ist die Datensicherung und Datensicherheit mehr und mehr in das Interesse der Internetnutzer gelangt. Dies kommt zum einen nicht nur durch die Ereignisse des 11. September 2001, sondern auch dadurch dass Angriffe auf unternehmensinterne Computernetze (Hackerangriffe) immer häufiger werden.[1] Da die kommerzielle Nutzung des Internet in den letzten Jahren ohnehin ein ständiges Wachstum erfahren hat,[2] so dass die Abwicklung von Rechtsgeschäften über das Internet immer selbstverständlicher wird,[3] fällt die Sicherheit und Sicherung sowohl des Dateninhalts als auch der persönlichen Daten der einzelnen Nutzer um so schwerer ins Gewicht. Unternehmen suchen nach Möglichkeiten, um die Vorteile eines flexiblen Internets in Einklang mit steigenden Sicherheitsanforderungen zu bringen.

Als neue Dienstleistungsform für eine sichere Unternehmenskommunikation haben sich Virtuelle Private Netzwerke (VPN) herausgebildet, denen immer mehr wirtschaftliche Bedeutung zukommt,[4] und die erst in den letzten zwei bis drei Jahren in der juristischen Fachliteratur Erwähnung finden.[5]
Im Allgemeinen wird ein VPN heutzutage als ein Netz von Verbindungen definiert, die über ein öffentliches Netzwerk, wie dem Internet aufgebaut

[1] Frankfurter Allgemeine Zeitung vom 21. Januar 2002, S. 23; Frankfurter Allgemeine Zeitung vom 21. März 2002, S. 21; Frankfurter Allgemeine Zeitung vom 11. April 2002, S. 22; Frankfurter Allgemeine Zeitung vom 27. Januar 2003, S. 22; Frankfurter Allgemeine Zeitung vom 10. Februar 2003, S. 15.
[2] Hobert, Datenschutz und Datensicherheit im Internet, S. 31.
[3] Glatt, Vertragsschluss im Internet, S. 13.
[4] Dem VPN-Markt in Europa wird auch zukünftig ein kräftiges Wachstum bescheinigt. Für 1999 wurde eine Marktgröße von ca. 85 Millionen US-$ festgestellt; das jährliche Marktwachstum soll zwischen 1996 und 2006 bei durchschnittlichen 45,1% liegen (vgl. auch Campo/Pohlmann, Virtual Private Networks, S. 35). Siehe ebenso Frankfurter Allgemeine Zeitung vom 23. August 2004, S. 17, wo darauf verwiesen worden ist, dass Schweizer Banken mit Virtuellen Privaten Netzwerken arbeiten.
[5] Vgl. Imping in: Spindler, Vertragsrecht der Telekommunikations-Anbieter, Teil II Rn. 3; Roth/Haber, ITRB 2004, 19 ff.; Schumacher, CR 2006, S. 229 ff., der VPN als eine neue Form des Unternehmensnetzwerkes bezeichnet.

werden, sich aber für den Nutzer durch die Verwendung spezieller Technik[6] wie private Leitungen darstellen.[7] Die ursprüngliche Bedeutung der Bezeichnung „Virtuelles Privates Netzwerk“ ist dabei auf ein VPN beschränkt, das auf dem Internet-Protokoll IP basiert, wobei dem Internet aufgrund seiner flächendeckenden Verfügbarkeit die größte Bedeutung zukommt.[8] Daher soll auch im Rahmen dieser Arbeit ein Internet-VPN (nachfolgend: VPN) Gegenstand der Untersuchung sein, insbesondere um Datenschutz im Internet untersuchen zu können.

Technische Details werden im zweiten Abschnitt dieser Arbeit behandelt, wobei vorab das folgende Bildbeispiel eines Netzwerkes zum besseren Verständnis beitragen soll.



Mittels eines VPN können verschiedene Standorte, etwa Tochterunternehmen, Zweigstellen, Telearbeiter (im häuslichen Umfeld) oder Externe (beispielsweise Lieferanten oder freie Mitarbeiter, die nicht im Betrieb eingebunden sind) netztechnisch miteinander verbunden[9] und/oder diesen kann der Zugriff auf den Zentralrechner eines Unternehmens ermöglicht werden.[10] Die Anbindung von Externen wird auch als Extranet-VPN bezeichnet.[11]

---

[6] Siehe hierzu den zweiten Abschnitt dieser Arbeit, insbesondere S. 44 ff.

[7] Buckbesch/Köhler, Virtuelle Private Netze, S. 11. Siehe auch Böhmer, Virtual Private Networks (2. Auflage), S. 6, der ein VPN als ein Netz von Verbindungen zur Übermittlung von privaten Daten/Informationen bzw. Datenverkehr bezeichnet.

[8] Siehe hierzu Buckbesch/Köhler, Virtuelle Private Netze, S. 12.

[9] Siehe hierzu etwa directVPN Administrator – Benutzerhandbuch, Stand Oktober 2005, S. 14 (abrufbar unter www.t-online.de/directVPN bzw. ftp://software.t-online.de/pub/service/pdf/directVPN_Benutzerhandbuch_Admin.pdf, Website vom 30.09.2006, im Folgenden: „directVPN Administrator-Benutzerhandbuch“), wo ausgeführt wird, dass ein Benutzer nach der erfolgreichen Anmeldung am directVPN mit anderen angemeldeten Computern Daten austauschen kann.

[10] Siehe außerdem das Bildbeispiel auf S. 44, wobei unter Verwendung der entsprechenden Techniken gleichfalls möglich ist, nicht nur den Zugriff auf einen zentralen Unternehmensserver, sondern auf jedwede Stelle bzw. jedweden Standort im VPN zu erlauben (vgl. S. 55).

[11] Vgl. Lipp, VPN, S. 43; Buckbesch/Köhler, Virtuelle Private Netze, S. 16. Bei der Extranet-Variante gibt es eine Vielzahl interessanter Anwendungsfälle, wie beispielsweise die

Ein VPN, welches in bzw. von einem Unternehmen eingesetzt wird, beinhaltet dementsprechend die Vernetzung unterschiedlicher Standorte oder Personen mit dem Ziel, ein Arbeiten zu ermöglichen, wie es auch ohne räumliche Trennung möglich wäre. Hierbei kann ein Anbieter seinem Kunden ein VPN mit mehr oder weniger eigener Beteiligung bereitstellen. Ein VPN ermöglicht, dass sensible Daten während der Übertragung über verschiedene, sicherheitstechnisch nicht einschätzbare Netzwerke (wie das Internet), vertrauenswürdig übertragen werden, so dass nur die dazu berechtigten Organisationen oder Personen auf die zu schützenden Daten zugreifen und ihren Informationsgehalt verändern können.[12]

So bieten viele VPN-Anbieter[13] ihren Kunden neben der Bereitstellung eines Internetzugangs an sämtlichen Standorten[14] und spezieller VPN-Technik (Soft- und/oder Hardware) die Administration der technischen Systeme im VPN an.[15] Regelmäßig ist damit als Zusatzleistung das Angebot eines E-Mail-Service

---

Möglichkeit für Lieferanten die Logistikdatenbank einzusehen (siehe Buckbesch/Köhler, Virtuelle Private Netze, S. 16). Siehe zum Begriff des Extranet auch Rudloff in: Gounalakis, Rechtshandbuch Electronic Business, § 1 Rn. 130.

[12] Siehe auch das Bildbeispiel von Böhmer, Virtual Private Networks (2. Auflage), S. 2 in welchem der Informationsaustausch zwischen zwei Unternehmensstandorten über das Internet dargestellt wird und die damit verbundene enorme Zeitersparnis, die mit einem Arbeiten zwischen zwei an einem Ort ansässigen Nachbarbüros vergleichbar ist (vgl. hierzu auch Buckbesch/Köhler, Virtuelle Private Netze, S. 15, der einen Vergleich dahingehend zieht, dass ein Arbeiten möglich ist, als wenn der Nutzer an das Firmennetz lokal angeschlossen wäre).

[13] Siehe die Angebote von T-Online zu unterschiedlichen Realisierungsmöglichkeiten eines VPN, abrufbar unter www.t-online.de/directVPN sowie ftp://software.t-online.de/pub/service/business/cs/vpn/securevpn-benutzerhandbuch.pdf (Websites vom 30.09.2006). T-Online bietet zur Zeit hauptsächlich zwei unterschiedliche Produkte an, die neben der Bereitstellung eines Internetzugangs zum einen das Angebot von VPN-Technik in Form von Hardware sowie Software (ftp://software.t-online.de/pub/service/business/cs/vpn/securevpn-benutzerhandbuch.pdf) und zum anderen (neben der Bereitstellung eines Internetzugangs) allein das Angebot von VPN-Software beinhalten (www.t-online.de/directVPN). Bei dem ersten Angebot werden bei der Realisierung des VPN zudem weitere Dienstleistungen angeboten, die im Verlauf dieser Arbeit (insbesondere im technischen Teil) dargestellt und behandelt werden.

[14] Im Hinblick auf Externe oder Telearbeiter, die im eigenen häuslichen Bereich tätig sind, wird in dieser Arbeit jedoch berücksichtigt, dass diese oftmals eigene Verträge mit dem Provider bezüglich eines Internetzugangs abschließen, da ein Internetzugang in diesen Fällen regelmäßig nicht ausschließlich nur für Zwecke des VPN genutzt wird.

[15] Vgl. außerdem die VPN-Angebote von Arcor AG & Co.KG abrufbar unter http://www.arcor.de/business/soho/netzwerk/sec_high.jsp; Cable & Wireless Telecommunication Services GmbH abrufbar unter http://www.cw.com/europe/services/internet_vpn.html und http://www.cw.com/docs/services/product_pdfs/internet_vpn.pdf; Level 3 Communications GmbH abrufbar unter http://www.level3.com/3248.html; QSC AG abrufbar unter http://www.qsc.de/?referrer=Q-DSLhome sowie http://www.qsc.de/de/isp_und_carrier/qsc-speedw@y-shdsl/aufbau_von_vpn/indexCOLT TELECOM GmbH abrufbar unter http://www.colt.net/de/ge/produkte/data_/colt_ip_vpn_corporate; Freenet AG abrufbar unter http://www.freenet-business.de/loesungen/vpn/vpn.phpoder von Claranet GmbH abrufbar unter http://www.claranet.de./ipservices/vpn/ (Websites vom 30.09.2006).

erfasst.[16]

Ein solches Komplett-Angebot bzw. kombinierter Dienst[17] bildet den Schwerpunkt dieser Arbeit,[18] und es soll in einer Gesamtschau der Beteiligtenverhältnisse untersucht werden, wie sich die datenschutzrechtlichen Verpflichtungen der einzelnen Beteiligten voneinander abgrenzen lassen und welche Wechselwirkungen bestehen, was bislang noch nicht Gegenstand einer juristischen Arbeit gewesen ist: Bei VPN-Rechtsbeziehungen treffen die Rechtssphären der Auftraggeber und deren Nutzer (Arbeitnehmer) mit denen der VPN-Anbieter sowie mit denen der Personen zusammen, deren Daten erhoben, verarbeitet und genutzt werden.[19]

---

[16] Siehe zum E-Mail-Dienst als Nebenleistung des Access-Providers auch Cichon, Internetverträge Rn. 121 ff.; Schneider, Verträge über Internet-Access, S. 97. Siehe außerdem Böhmer, Virtual Private Networks (2. Auflage), S. 364, der verschiedene VPN-Kategorien tabellarisch auflistet und dabei den E-Mail-Dienst in jeder der Kategorien als typische Mindestanforderungen begreift.

[17] Siehe zu dem Begriff „Komplettpaket" auch Schuster in: TKG-Kommentar (2. Auflage), § 4 TKG Rn. 4a. In der neuen Auflage des TKG-Kommentars (3. Auflage) wird nun der Begriff „Kombinationspaket" verwendet (Gersdorf in: TKG-Kommentar (3. Auflage), Einleitung C Rn. 23). Siehe zum kombinierten Dienst auch Wittern/Schuster in: TKG-Kommentar (3.Auflage), § 3 TKG Rn. 49.

[18] Die Aufteilung der Leistungen zwischen einzelnen Personen kann aber noch weitergehen. So kann unter Umständen an jedem einzelnen Standort für jede einzelne Leistung ein anderer Anbieter in Betracht kommen. Außerdem gibt es Anbieter, die lediglich Hard- und Softwaresysteme für ein VPN bereitstellen, ohne aber selbst Anbieter von Internet-Zugängen zu sein (siehe etwa die Angebote von HOB GmbH & Co. KG abrufbar unter www.hob.de und http://www.hob.de/produkte/connect/rd_vpn.jsp
sowie von 3COM GmbH abrufbar unter www.3com.de und
http://www.3com.com/network/vpn.html, beide Websites vom 30.09.2006).

[19] Siehe Jandt, MMR 2006, 652 ff. mit Beispielen zu weiteren Diensten, denen ein Mehrpersonenverhältnis zugrunde liegt (Geschenkservice für digitale Produkte, Located Based Services zur Statusüberwachung von Personen).

B. Ziel der Untersuchung

Im Wesentlichen verfolgt diese Arbeit die folgenden zwei Ziele:

Ziel 1: Untersuchung der „Relevanz des Mehrpersonenverhältnisses“ im Rahmen einer datenschutzrechtlichen Prüfung

Es soll in einer vergleichenden Gesamtschau der Personenverhältnisse ermittelt werden, welche datenschutzrechtlichen Pflichten in den einzelnen Personenverhältnissen bestehen und ob sich die rechtliche Einordnung von Diensten und Daten in Abhängigkeit vom jeweils betrachtenden Personenverhältnis innerhalb eines kombinierten Dienstes ändern kann. Damit ist die Frage verbunden,

- ob eine pauschale rechtliche Einordnung von Diensten und Daten gerechtfertigt ist oder
- ob für eine rechtliche Bewertung stets die Betrachtung des Mehrpersonenverhältnisses sowie der jeweiligen Personenverhältnisse erforderlich sind.

Ziel 2: Untersuchung der „Relevanz der Technik“ Im Rahmen einer datenschutzrechtlichen Prüfung

Es soll der Einfluss der Technik auf die rechtliche Einordnung von Diensten und Daten untersucht und die Frage beantwortet werden, ob moderne Techniken und komplexe technische Systeme das Recht beeinflussen können. Im Mittelpunkt der Betrachtung steht,

- ob die rechtliche Einordnung von Diensten und Daten allein auf Grundlage der Technik gerechtfertigt ist,
- ob die rechtliche Einordnung eines Dienstes zwangsläufig auch die (datenschutz)rechtliche Einordnung von Daten präjudiziert oder ob

darüber hinaus die Datenverarbeitung auf dem jeweiligen technischen System zu untersuchen ist.

- welche technischen (Hardware)Systeme innerhalb eines VPN vorhanden sind und wer letztendlich die Verantwortung für das technische System einerseits sowie die Verantwortung für (die auf dem System stattfindende) Datenverarbeitung andererseits trägt

Die beiden Zielsetzungen erfordern im Verlauf der Arbeit ebenso eine Auseinandersetzung mit Fragen des Arbeitsverhältnisses, Arbeitnehmerdatenschutzes und Telearbeit sowie eine Abgrenzung zwischen Funktionsübertragung und Auftragsdatenverarbeitung.

Die nachfolgenden Ausführungen unter „I. Relevanz des Mehrpersonenverhältnisses?“ und „II. Relevanz der Technik?“ beinhalten zunächst einen Überblick der gesetzlichen Grundlagen sowie ergänzende Erläuterungen zur Bedeutung des Themas.

I. Relevanz des Mehrpersonenverhältnisses?

Die aufgeworfene Fragestellung, ob sich die rechtliche Einordnung von Diensten und Daten in Abhängigkeit vom jeweils betrachtenden Personenverhältnis innerhalb eines kombinierten Dienstes[20] ändert und welche datenschutzrechtlichen Pflichten in den einzelnen Personenverhältnissen bestehen, lässt sich mittels eines VPN aus dem Grunde gut abbilden, da hier unterschiedliche Interessensphären zu berücksichtigen und miteinander in Einklang zu bringen sind.
So hat derjenige, der das VPN initiiert, als VPN-Auftraggeber eigene Interessen,[21] muss aber gleichzeitig die Interessen des Nutzers (der auch ein Arbeitnehmer sein kann) und die Interessen desjenigen, dessen Daten etwas aufgrund einer Kundenbeziehung verarbeitet werden, beachten. Darüber hinaus verarbeitet ebenso der (kommerzielle) Dienstleister, der das VPN bereitstellt,

[20] Siehe S. 5.
[21] Siehe beispielsweise zum Recht der Protokollierung Bizer, DuD 2006, S. 270 ff., insbesondere S. 272 zur systemseitigen Erhebung der Protokolldaten ohne aktive Mitwirkung des Betroffenen.

Daten von VPN-Auftraggeber, Nutzer und dem Betroffenen, wobei er gegebenenfalls für seine Diensterbringung wiederum auf weitere Dienstleister zurückgreifen muss.

Es geht somit nicht nur um die Sicherung der Rechte eines Arbeitnehmers und eines Arbeitgebers bzw. VPN-Auftraggebers, dessen Tätigkeit als Unternehmer wesentlicher Bestandteil seines Persönlichkeitsrechts ist,[22] sondern auch um die Interessen eines Dritten, dessen Daten „online" verarbeitet werden. Es kann sich insoweit bei einem VPN um eine Konstruktion zu Lasten Dritter handeln, sofern dessen Interessen bei der Datenverarbeitung nicht angemessen berücksichtigt werden.[23] Aufgrund der Arbeitnehmerrechte sind darüber hinaus ebenso die Beteiligungsrechte des Betriebsrates zu berücksichtigen.[24]

Daher stellt zum einen die seitens des Bundesverfassungsgerichts betonte informationelle Selbstbestimmung als Funktionsbedingung der Demokratie auch in einem VPN ein wesentliches Merkmal dar, das erfüllt werden muss.[25]
Zum anderen ist es aufgrund der wirtschaftlichen Bedeutung und der Komplexität von VPN besonders wichtig, nicht erst in der Betriebs- sondern bereits in der Planungsphase die einzelnen rechtlichen Verantwortungsbereiche und datenschutzrechtlichen Pflichten der unterschiedlichen Beteiligten voneinander abzugrenzen.
Es wird daher in jedwedem Personenverhältnis innerhalb eines VPN geprüft, ob die datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes (BDSG),[26] Teledienstedatenschutzgesetzes (TDDSG),[27] oder der §§ 91 ff. des

[22] Vgl. Raffler/Hellich, NZA 1997, 862, 862. Siehe hierzu auch Boemke/Ankersen, BB 2000, 1570 ff., zum Schutz der betrieblichen Daten des Arbeitgebers S. 1572.
[23] Vgl. in diesem Zusammenhang auch von Lewinski, NJW 2004, 349, 349.
[24] Vgl. hierzu auch Wedde, Telearbeit, S. 191 ff. Siehe außerdem Boemke/Ankersen, BB 2000, 2254, 2255/2256 zum allgemeinen Unterrichtungsanspruch des Betriebsrates gemäß § 80 Abs. 2 BetrVG.
[25] Vgl. zum informationellen Selbstbestimmungsrecht BVerfGE 65, 1, 42.
[26] Bundesdatenschutzgesetz vom 20.12.1990 (BGBl. I S. 2954), neu gefasst durch Artikel 1 Nr. 13 Gesetz vom 18.5.2001, BGBl. I S. 904 mit Wirkung vom 23.5.2001, zuletzt geändert durch Gesetz vom 21.08.2002 (BGBl. I S. 3322). Siehe zur Novellierung des BDSG auch Gola/Klug, NJW 2001, 3747 ff. sowie Gola/Klug, Grundzüge des Datenschutzrechts, S. 10 ff.
[27] Das TDDSG ist enthalten im Gesetz zum elektronischen Geschäftsverkehr – EGG, veröffentlicht am 20.12.2001, BGBl. I S. 3721. Mit dem EGG wird die europäische Richtlinie über den elektronischen Geschäftsverkehr durch Änderungen des TDG und der ZPO umgesetzt. Die Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs im Binnenmarkt (ABl. EG Nr. L 178 vom

Telekommunikationsgesetzes (TKG),[28] letzteres unter Berücksichtigung der Datenschutzrichtlinie für elektronische Kommunikation,[29] im Folgenden: EU-Richtlinie 2002/58/EG,[30] anwendbar sind.

17.7.2000, S. 1), E-Commerce-Richtlinie, war bis zum 17.1.2002 in nationales Recht umzusetzen mit dem Ziel, bestimmte für die Dienste der Informationsgesellschaft geltende innerstaatliche Regelungen anzugleichen – vgl. Artikel 1 Abs. 2 der Europäischen Richtlinie. Siehe auch Gesetzesbeschluss des Deutschen Bundestages über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 9.11.2001, BR-Drucks. 912/01. Siehe zum novellierten TDDSG auch Geis, CR 2002, 667 ff. Außerdem Gola/Klug, Grundzüge des Datenschutzrechts, S. 187 mit dem Hinweis, dass das TDDSG neben dem TDG und dem Mediendienste-Staatsvertrag (siehe zu letzterem Fn. 33) der Bundesländer zu der so genannten Multimediagesetzgebung zählt, mit der insbesondere Datenschutzprobleme der Internetnutzung angegangen werden sollten.

[28] Das Telekommunikationsgesetz vom 25.7.1996, BGBl. I S. 1120, geändert durch Artikel 2 Abs. 6 Sechstes Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen vom 26.8.1998, BGBl. I S. 2521, ist überarbeitet worden, wobei die Regelungen der Telekommunikationsdiensteunternehmen-Datenschutzverordnung (TDSV, Telekommunikationsdiensteunternehmen-Datenschutzverordnung vom 18.12.2000, BGBl. I S. 1740) nunmehr vollständig in den §§ 91 ff. TKG enthalten sind (siehe auch TKG vom 22.04.2004, BGBl. I S. 1190). Siehe zum Änderungsgesetz des TKG im Kabinettsentwurf vom 17.05.2006 (TKGÄndG) die Stellungnahme des Bundesrates (BR-Drs. 359/1/06) sowie Klaes, MMR 2006, 641, 641. Die Frist für die Umsetzung der TKG-Novelle war zwar bereits am 24.07.2003 abgelaufen, der Entwurf ist aber erst am 01.07.2004 in nationales Recht umgesetzt worden. Hierbei wurden bislang geltende Begrifflichkeiten wie „Verbindungsdaten" gemäß § 2 Nr. 4 TDSV durch „Verkehrsdaten" (siehe § 3 Nr. 30 TKG) ausgetauscht. Diese Begriffe sollen aber nach dem Willen der Bundesregierung gleichbedeutend sein und die Terminologie im Zuge der europarechtlichen Harmonisierung und Vereinheitlichung angepasst werden, vgl. außerdem Ladeur, K&R 2003, 153, 155. Des Weiteren wird die Bezeichnung „Kunde" (§ 2 Nr. 1a) TDSV) durch „Teilnehmer" (§ 3 Nr. 20 TKG) ersetzt und meint damit diejenige natürliche oder juristische Person, die eine Dienstleistung beim Diensteanbieter beauftragt. Vgl. zur verspäteten Umsetzung des EU-Richtlinienpakets vom 07.03.2002 (bestehend aus Rahmen-; Genehmigungs-, Zugangs- und Universaldienstrichtlinie) Ellinghaus, CR 2003, 657 ff., der in CR 2004, 23, 23 darauf verweist, dass eines der wesentlichen Ziele der TKG-Novelle die europarechtskonforme Umsetzung der zwingenden Vorschriften des EU-Richtlinienpakets ist (Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 07.03.2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) (ABl. EG Nr. L 108 vom 24.04.2002, S. 33); Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 07.03.2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Genehmigungsrichtlinie) (ABl. EG Nr. L 108 vom 24.04.2002, S. 21); Richtlinie 2002/19/EG des Europäischen Parlaments und des Rates vom 07.03.2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (Zugangsrichtlinie) (ABl. EG Nr. L 108 vom 24.04.2002, S. 7); Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 07.03.2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie) (ABl. EG Nr. L 108 vom 24.04.2002, S. 51) sowie Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie) (ABl. EG Nr. L 201 vom 31.07.2002, S. 37).

[29] EU-Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation des Europäischen Parlaments und des Rates vom 12.07.2002 (ABl. EG Nr. L 201 vom 31.07.2002, S. 37). Diese sollte ursprünglich seitens der Mitgliedstaaten vor dem 31.10.2003 umgesetzt werden (Artikel 17 der EU-Richtlinie 2002/58/EG) und geht davon aus, dass bei der Verarbeitung personenbezogener Daten bei öffentlich zugänglichen elektronischen Kommunikationsdiensten in öffentlichen Kommunikationsnetzen noch Regelungsbedarf besteht (siehe zur Fristsetzung bis zum 31.10.2003 auch Gola/Klug, Grundzüge des Datenschutzrechts, S. 197). Durch die Vorgaben der EU-Richtlinie 2002/58/EG sind die neuen Begriffe des „öffentlich zugänglichen

Hierbei müssen ebenso die jeweils zugrundeliegenden Dienste unter das TKG[31] oder unter das Teledienstegesetz (TDG)[32] eingeordnet werden.Der Mediendienste-Staatsvertrag (MDStV) ist in dieser Arbeit von geringerer Bedeutung und findet daher nur am Rande Erwähnung.[33]

---

elektronischen Kommunikationsdienstes“ und des „öffentlichen Kommunikationsnetzes“ eingeführt worden. Eine Definition zu diesen beiden Begrifflichkeiten liefert die Richtlinie nicht. Aber im Zuge europaweiter Harmonisierung geht es auch hier (vgl. bereits Fn. 28) im Wesentlichen um die Vereinheitlichung und Anpassung der Terminologie (siehe hierzu insbesondere Ladeur, K&R 2003, 153, 153). Mit dem Begriff des öffentlichen Kommunikationsnetzes ist zumindest auch das Internet gemeint (vgl. hierzu auch Eckhardt, CR 2003, 805, 805).

[30] Gemäß Artikel 2 Abs. 2 S. 1 der EU-Richtlinie 2002/58/EG stellen die enthaltenen Regelungen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die Harmonisierung der Vorschriften der Mitgliedstaaten dar (EU-Richtlinie des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ABl. EG Nr. L 281 vom 23.11.1995, S. 31.), die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten. Datenschutz als Gemeinschaftsaufgabe der Europäischen Union wurde im Übrigen erstmals im Jahre 1990 ausdrücklich anerkannt, nachdem sich allgemein (mit Ausnahme Griechenlands und Italiens) die Forderung nach klaren restriktiven Bestimmungen bezüglich des Schutzes von personenbezogenen Daten durchgesetzt hatte, vgl. hierzu Dammann/Simitis, EG-Datenschutzrichtlinie, S. 62/63. Siehe zur Umsetzung der EU-Datenschutzrichtlinie Brühann, RDV 1996, 12 ff., der darauf verweist, dass die Umsetzung der völlig anderen Grundstruktur erhebliche Änderungen im BDSG erfordert (Brühann, RDV 1996, 12, 15).

[31] In der Neufassung des TKG ist der Begriff „Telekommunikationsdienstleistung“ (§ 3 Nr. 18 TKG a.F.) durch „Telekommunikationsdienst“ (§ 3 Nr. 24 TKG) ausgetauscht worden. Diese Definition entspricht laut der Begründung zum Gesetzesentwurf des TKG vom 15.10.2003 (nachfolgend: TKG-E, abrufbar unter http://www.computerundrecht.de/docs/tkg_e_entwurf_mit_begruendungpropertypdf.pdf, Website vom30.09.2006), S. 80, Artikel 2c S. 1 der Rahmenrichtlinie (Richtlinie 2002/21/EG des europäischen Parlaments und des Rates vom 07.03.2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste, ABl. Nr. L 108 vom 24.04.2001, S. 33). Allerdings ist insoweit eine Änderung erfolgt, dass in der jetzigen Begriffsdefinition „Telekommunikationsdienst“ der Begriff der Gewerblichkeit gestrichen ist, so dass damit nicht nur kommerzielle Anbieter erfasst sind. Denn nunmehr ist eindeutig klargestellt, dass „Telekommunikationsdienste in der Regel gegen Entgelt erbrachte Dienste“ sind (siehe Zimmer, CR 2003, 893, 896, die darauf verweist, dass der Gesetzgeber bewusst auf die Gewerblichkeit verzichtet hat). Die EU-Richtlinie 2002/58/EG führt darüber hinaus den Begriff des „Dienstes mit Zusatznutzen“ ein (Artikel 2 g) der EU-Richtlinie 2002/58/EG). Damit ist jeder Dienst gemeint, der über das für die Übermittlung einer Nachricht oder Fakturierung dieses Vorganges erforderliche Maß hinausgeht (Erwägungsgrund 18 der EU-Richtlinie 2002/58/EG nennt als Beispiele Verkehrsinformationen oder die Wettervorhersage). Daher wird in dieser Arbeit ebenso die Frage behandelt werden (S. 102 ff.), ob dieser Begriff der derzeit geltenden gesetzlichen Definition des Teledienstes im Sinne des Teledienstesgesetzes entspricht.

[32] Auch das Teledienstegesetz (TDG), welches Regelungen zu Telediensten enthält, ist im Gesetz zum elektronischen Geschäftsverkehr – EGG enthalten, veröffentlicht am 20.12.2001 im BGBl. I S. 3721. Siehe auch S. 7 Fn. 27.

[33] Siehe 9. Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag) vom 20. Januar bis 7. Februar 1997, in Kraft getreten am 01.08.1997 (HessGVBl. I S. 134 ff.; BremGBl. I, S. 205 ff.), zuletzt geändert durch Art. 8 Achter Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (Achter Rundfunkänderungsstaatsvertrag) vom 08. bis 15. Oktober 2004 (HessGVBl.2005, S. 118 ff.; BremGBl. 2005, S. 35 ff.). Der Zweck des MDStV besteht darin, in

Diese Abgrenzung zwischen TKG und TDG ist insbesondere wichtig, da häufig juristische Personen oder rechtsfähige Personengesellschaften ein VPN beauftragen und gemäß § 91 Abs. 1 S. 2 TKG (abweichend vom allgemeinen Datenschutzrecht)[34] auch dem Fernmeldegeheimnis gemäß § 88 TKG unterliegende Einzelangaben von juristischen Personen den personenbezogenen Daten gleichstehen. Damit sind ebenso die datenschutzrechtlichen Regelungen der §§ 91 ff. anwendbar sind.[35]
Dem Schutzbereich des BDSG und des TDDSG unterliegen dagegen ausschließlich natürliche Personen,[36] wobei darüber hinaus keine Pflichten zur Wahrung des Fernmeldegeheimnisses normiert sind.[37]

---

allen Ländern einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen (§ 1 MDStV). Der MDStV hat den Btx-Staatsvertrag vom 31.08.1991 außer Kraft gesetzt (Knothe, AfP 1997, 494, 495, der darauf verweist, dass der MDStV eine Weiterentwicklung des Btx-Staatsvertrages darstellt; siehe zum Mediendienste-Staatsvertrag auch die Ausführungen von Gounalakis, NJW 1997, 2993 ff. sowie Ritz, Inhalteverantwortlichkeit von Online-Diensten, S. 66 ff).

[34] Nach § 3 Abs. 1 BDSG gilt das Datenschutzgesetz nur für natürliche Personen, nicht dagegen für juristische Personen (Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 17; Gola/Schomerus, BDSG, § 3 BDSG Rn. 11; zum allgemeinen Persönlichkeitsschutz einer Kapitalgesellschaft siehe auch BGH, RDV 1994, 181 ff.; OLG Karlsruhe, DuD 1983, 229, 230. Siehe im Übrigen auch Lewinski, DuD 2000, 39 ff., der insbesondere auf S. 40 ff. seine These begründet, dass eine Gleichbehandlung von Wirtschaftssubjekten nicht nur dadurch erreicht werden kann, Unternehmen ebenso dem Schutz der Datenschutzgesetze zu unterstellen, sondern auch dadurch, Einzelkaufleute und Freiberufler aus dem Schutzbereich der Datenschutzgesetze heraus zu nehmen.

[35] Siehe zum Schutzbereich des Fernmeldegeheimnisses als „Jedermanns-Grundrecht" insbesondere Groß in: Roßnagel, Handbuch Datenschutzrecht, 7.8 Rn. 7. Siehe auch Holznagel/Enaux/Nienhaus, Grundzüge des Telekommunikationsrechts, S. 190. Hier wird angemerkt, dass Fernmeldegeheimnis und Datenschutz vielfache Überschneidungsbereiche aufweisen. So ist beispielsweise die Information, wer an einem Kommunikationsvorgang beteiligt ist, sowohl durch das Fernmeldegeheimnis als auch durch das Recht auf informationelle Selbstbestimmung geschützt. Eine genaue Trennung zwischen den beiden Schutzbereichen ist oft nicht möglich, wobei auch das TKG selbst zwischen Datenschutz und dem Fernmeldegeheimnis keinen deutlichen systematischen Unterschied macht (Holznagel/Enaux/Nienhaus aaO). Siehe dieselben zum Schutzgut des Fernmeldegeheimnisses außerdem in: Telekommunikationsrecht, Rahmenbedingungen – Regulierungspraxis, Rn. 643.

[36] Vgl. auch Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 255 sowie Wegel, Presse und Rundfunk im Datenschutz, S. 24 und der Ausführung, dass Daten von juristischen Personen nur dann dem Datenschutzrecht unterfallen, wenn ein Personenbezug erkennbar ist. In der seit 2001 geltenden Fassung des TDDSG ist in §§ 1 Abs. 1 und 2 Nr. 2 ausdrücklich klargestellt worden, dass das TDDSG nicht für die Daten der juristischen Personen gilt, sondern sich lediglich auf den Schutz personenbezogener Daten beziehen. In § 2 Nr. 2 TDDSG wurden zu diesem Zweck die Wörter „oder juristische" gestrichen. Begründet liegt diese Änderung in § 3 BDSG, der ausdrücklich regelt, dass personenbezogene Daten Einzelangaben natürlicher Personen sind. So wird nun auch das Missverständnis aus dem Weg geräumt, welches dadurch entstanden ist, dass das TDG auch Geltung für juristische Personen hat (vgl. hierzu etwa v.Rottenburg, WM 1997, 2381, 2386). Allerdings scheint Bock in: Bräutigam/Leupold, B VII Rn. 134 auch nach der Änderung des TDDSG immer noch anderer Auffassung zu sein. Dennoch ist die Gesetzesneufassung eindeutig.

[37] Der Telediensteanbieter ist gesetzlich nicht zur Einhaltung des Fernmeldegeheimnisses verpflichtet, da das Fernmeldegeheimnis ausschließlich für Telekommunikationsdienste in § 88 TKG geregelt wird. Vgl. auch Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDDSG

Aber nur derjenige, der zur Wahrung des Fernmeldegeheimnisses verpflichtet ist, ist nach § 88 Abs. 2 TKG an die zweckgebundene Verwendung der Kenntnisse gebunden und kann gemäß § 206 Abs. 1 StGB mit Freiheitsstrafe bis zu fünf Jahren bestraft werden, sofern er unbefugt einer anderen Person Mitteilung über Tatsachen macht, die dem Fernmeldegeheimnis unterliegen.[38] Das BDSG enthält zwar gemäß §§ 43 Abs. 2 Nr. 1, 44 BDSG ebenfalls Strafvorschriften für den Fall, dass jemand unbefugt personenbezogene Daten an einen Dritten weitergibt oder dem Dritten die Möglichkeit gibt, solche Daten einzusehen oder abzurufen.[39] Jedoch liegt gemäß § 44 Abs. 1 BDSG das Strafmaß bei höchstens zwei Jahren, wobei zusätzlich erforderlich ist, dass der Täter gegen Entgelt handelt oder in der Absicht, sich oder einen anderen zu bereichern.[40] Außerdem ist zu berücksichtigen, dass das § 9 TDDSG abschließende Bußgeldvorschriften enthält, so dass bei Telediensten kein Rückgriff auf die Strafbarkeitsregelungen des BDSG möglich ist.[41]

Wichtig ist die Unterscheidung zwischen den Pflichten des TKG und TDDSG darüber hinaus für behördliche Zuständigkeitsfragen. Die Regulierungsbehörde, die seit dem 13.07.2005 in Bundesnetzagentur umbenannt ist, kann bei Nichterfüllung von datenschutzrechtlichen Verpflichtungen gemäß § 115 Abs. 1 TKG konkrete Anordnungen treffen,[42] um die Einhaltung der Vorschriften des siebten Teils des TKG, also ebenso des Fernmeldegeheimnisses, sicherzustellen, und darüber hinaus den Betrieb der betreffenden Telekommunikationsanlage oder das Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise gemäß § 115 Abs. 3 TKG untersagen.
Der Bundesbeauftragte für den Datenschutz, der hier anders als bei Telediensten zuständig ist (§ 115 Abs. 4 TKG), richtet seine Beanstandungen

---

Rn. 56, der ausführt, dass ein Telediensteanbieter zur Wahrung des Fernmeldegeheimnisses nur verpflichtet ist, soweit er zur Durchführung des Teledienstes auch geschäftsmäßig Telekommunikationsdienste gemäß § 3 Nr. 5 TKG a.F. erbringt.

[38] Vgl. auch Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDDSG Rn. 56.

[39] Vgl. auch § 3 Abs. 4 Nr. 3 BDSG, der den Tatbestand des Übermittelns regelt, sowie Gola/Schomerus, BDSG, § 3 BDSG Rn. 32.

[40] Darüber hinaus wird gemäß § 44 Abs. 2 BDSG die Tat nur auf Antrag verfolgt.

[41] Siehe Schmitz in: Spindler/Schmitz/Geis, § 9 TDDSG Rn. 2.

[42] Die Möglichkeit konkreter Anordnungen ergibt sich auch aus § 126 Abs. 2 TKG.

an die Bundesnetzagentur und übermittelt dieser nach pflichtgemäßem Ermessen weitere Ergebnisse seiner Kontrolle.[43]
Bei Telediensten sind hingegen gemäß § 38 Abs. 1 BDSG die Landesbehörden zuständig.[44]

Des Weiteren können nur Anbieter von Telekommunikationsdiensten den Pflichten des § 113 Abs. 1 TKG i.V.m. §§ 95, 111 TKG unterliegen und müssen den zuständigen Stellen, soweit im Sinne des Gesetzes erforderlich, unverzüglich Auskunft über ihre Kunden, etwa über deren Name und Adresse, erteilen.[45]
In § 113 Abs. 1 S. 2 TKG ist ferner geregelt, dass der Telekommunikationsdiensteanbieter ebenso zur Auskunft über Daten gemäß §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO verpflichtet ist, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird, insbesondere PIN und PUK.
Darüber hinaus besteht gemäß § 3 Abs.1 TKÜV[46] und gemäß § 3 Abs. 2 TKÜV i.V.m. § 100b Abs. 3 Satz 1 der Strafprozessordnung (StPO), des § 2 Abs. 1 Satz 3 des Artikel 10-Gesetzes (G-10-Gesetz) des § 23a Abs. 1 S. 1 des Zollfahndungsdienstegesetzes oder nach Landesrecht nur im Hinblick auf Telekommunikationsdienste und auf Anordnung die Verpflichtung zur Durchführung von Überwachungsmaßnahmen sowie zur Erteilung einer Auskunft über die näheren Umstände und gegebenenfalls Inhalt durchgeführter

[43] Vgl. Groß in: Roßnagel, Handbuch Datenschutzrecht, 7.8 Rn. 54 zur Zuständigkeit des Bundesdatenschutzbeauftragten neben der Bundesnetzagentur.
[44] Siehe hierzu Groß in: Roßnagel, Handbuch Datenschutzrecht, 7.8 Rn. 54. Siehe zum Verbot einzelner Verfahren durch die zuständigen Aufsichtsbehörden Gola/Schomerus, BDSG, § 38 BDSG Rn. 25/26.
[45] Vgl. auch Bäumler in: Roßnagel, Handbuch Datenschutzrecht, 8.3 Rn. 59, der ausführt, dass die Pflichten der Telekommunikationsgesetze nicht Internetprovider treffen, soweit sie Teledienste im Sinne von § 2 Abs. 2 Nr. 3 TDDSG anbieten.
[46] Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung - TKÜV) vom 3. November 2005 (BGBl. I S. 3136). Die Verpflichtungen aus der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22.06.1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. EG Nr. L 204 vom 21.07.1998, S. 37), geändert durch die Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20.07.1998 (ABl. EG Nr. L 217 vom 05.08.1998, S. 18), sind beachtet worden; siehe außerdem die entsprechende Ermächtigungsgrundlage in § 110 Abs. 2 TKG. Der Grundsatz der Vertraulichkeit des Fernmeldeverkehrs gilt in der gesamten europäischen Union. Sofern eine Überwachung nicht durch eine Rechtsvorschrift für spezifische Fälle und begrenzte Zwecke als notwendig zugelassen wird, ist sie rechtswidrig (vgl. Akmann in: Holznagel/Nelles/Sokol, TKÜV, S. 58).

Telekommunikation.[47] Ebenso ist gemäß § 113 Abs. 1 S. 3 TKG ein Zugriff auf die Daten, die dem Fernmeldegeheimnis gemäß § 88 TKG unterliegen, nur gemäß den einschlägigen gesetzlichen Vorschriften, also ebenso nur auf Anordnung, erlaubt.[48]
Die Anwendbarkeit des TKG führt insgesamt dazu, dass der Anbieter von Telekommunikationsdiensten und Telekommunikationsanlagen gemäß § 2 TKG den Regulierungsbefugnissen des Bundes unterliegt,[49] wobei die rechtlichen Anforderungen aus dem TKG hoch sind, und ihre Nichtbefolgung sanktioniert werden kann.[50]

Daher ist es sowohl für denjenigen, der sich für ein VPN entscheidet, als auch für denjenigen, der ein solches anbietet, ratsam, sich möglichst frühzeitig mit den rechtlichen Rahmenbedingungen auseinander zu setzen.

[47] Siehe Federrath in Holznagel/Nelles/Sokol, TKÜV, S. 117, der darauf hinweist, dass Teledienste nicht von den Pflichten der TKÜV betroffen sind. Vgl. zu den Kosten der TK-Überwachung Kube/Schütze, CR 2003, S. 663 ff. Siehe zur TKÜV ebenso Koch, Internet-Recht, S. 929.

[48] Vgl. insbesondere auch Ehmer in: TKG-Kommentar (2. Auflage), Anh § 88 TKG, der unter Anmerkung 1 (keine Randnummern vorhanden) ausführt, dass aus den Vorschriften des G-10-Gesetzes, der StPO und des Außenwirtschaftsgesetzes (AWG) (nun Zollfahndungsdienstegesetz) folge, dass der Gesetzgeber von der grundsätzlichen Verpflichtung, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, keine Ausnahmen vorgesehen hat. Lediglich hinsichtlich der Fragen, ob und in welchem Umfang für dieses Ermöglichen Vorkehrungen zu treffen sind, können Regelungen im TKG und in der TKÜV getroffen werden. Siehe zu den Maßnahmen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung ebenso Bock in: TKG-Kommentar (3. Auflage), § 110 TKG Rn. 12 ff. Siehe im Übrigen zur statistischen Entwicklung und zum rapiden Anstieg der Überwachungsmaßnahmen seit 1995 Jeserich in: Holznagel/Nelle/Sokol, TKÜV, S. 68; außerdem Kloepfer in: Holznagel/Nelles/Sokol, TKÜV, S. 100/101.Siehe zur gesetzlichen Verpflichtung zur Ermöglichung der Überwachung und Aufzeichnung auch Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 88 TKG(1998), Band 1, Rn. 7 ff. In diesem Sinne ebenso Holznagel/Enaux/ Nienhaus, Telekommunikationsrecht, Rahmenbedingungen – Regulierungspraxis, Rn. 708. Siehe zur Einschränkung des Fernmeldegeheimnisses auch K. Lau in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 88 TKG(2004), Band 2, Rn. 33 ff.

[49] Vgl. außerdem Telekommunikations-Kundenschutzverordnung (Telekommunikations-Kundenschutzverordnung (TKV) vom 11.12.1997 (BGBl. I S. 2910), geändert durch Verordnung vom 14.04.1999 (BGBl. I S. 705)).

[50] Vgl. Zimmer, CR 2003, 893, 898.

II. Relevanz der Technik?

Die Prüfung in dieser Arbeit, ob und welchen Einfluss die Technik auf die rechtliche Einordnung von Diensten und Daten haben könnte,[51] erfordert eine vertiefte Auseinandersetzung mit den technischen Grundlagen eines VPN.[52] Daher folgt im zweiten Abschnitt dieser Arbeit zunächst eine entsprechende ausführliche Darstellung.[53].

Insgesamt soll diese Arbeit ebenso eine Hilfestellung dafür geben, die Komplexität bei der Diensterbringung eines VPN aufzubrechen und zu zeigen, welche Daten auf welchen technischen Systemen anfallen können, um letztendlich den datenschutzrechtlichen Vorgaben gerecht werden zu können. Dabei darf im Besonderen nicht außer Betracht gelassen werden, wer für die Löschungspflichten verantwortlich ist und für die Sicherheit des technischen Systems Sorge zu tragen hat. Bezüglich der Erfüllung von technischen Schutzmaßnahmen enthält § 109 TKG unter Berücksichtigung des Artikels 4 der EU-Richtlinie 2002/58/EG besondere Regelungen.
Zu beachten ist, dass das TDDSG keine entsprechenden Regelungen enthält, so dass nur gemäß § 109 Abs. 1 TKG im Rahmen von Telekommunikationsdiensten Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogenen Daten sowie zur Abwehr von unerlaubten Zugriffen auf Daten- bzw. Telekommunikationsverarbeitungssystemen zu treffen sind, wobei die Bundesnetzagentur zur Umsetzung der Maßnahmen des § 109 TKG gemäß § 115 Abs. 2 Nr. 2 TKG entsprechenden Druck ausüben kann.[54]

Die Anwendbarkeit des TKG führt also dazu, technische und organisatorische Schutzvorkehrungen zur Verhinderung unbefugter Kenntnisnahmen von

---

[51] Siehe zum Ziel dieser Arbeit S. 5.
[52] Vgl. zur Bedeutung des technischen Wissen für den Juristen im Besonderen Sieber in: Hoeren/Sieber, Teil 1 Rn. 9 ff.
[53] Siehe S. 33 ff.
[54] Die Bundesnetzagentur kann nach § 115 Abs. 2 Nr. 2 TKG Zwangsgelder bis zu einhunderttausend Euro zur Durchsetzung der Verpflichtungen nach § 109 TKG festsetzen (siehe hierzu auch Zimmer, CR 2003, 893, 898). Diese Bußgeldvorschrift läuft auch seit der Neufassung des TKG nicht mehr ins Leere, da nunmehr die Höhe der Bußgelder gesetzlich festgelegt worden und nicht mehr einer (nicht umgesetzten) Verordnung vorbehalten sind (vgl. zu letzterem Groß in: Roßnagel, Handbuch Datenschutzrecht, 7.8 Rn. 21).

erhobenen und gespeicherten Daten der einzelnen Verbindungen zu treffen. Damit ist aber bei der Datenverarbeitung innerhalb eines VPN zu prüfen, ob und welche organisatorischen Anforderungen zu erfüllen sind, und ob bestehende Datenverarbeitungssysteme eventuell umorganisiert werden müssen.[55] Dementsprechend ist es auch hier wichtig, das Mehrpersonenverhältnis im Rahmen der Untersuchung in den Mittelpunkt zu stellen, da so festgestellt werden kann, wer im Einzelfall Anbieter im VPN und zu diesen organisatorischen Maßnahmen verpflichtet ist.

Im Hinblick auf die Frage, inwieweit die Technik das Recht beeinflusst, hat ein (jeweiliger) Diensteanbieter gemäß § 3a BDSG sein Angebot außerdem an dem Ziel auszurichten, keine oder jedenfalls so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.[56] Damit ist die Aufgabe verbunden, bereits durch die Gestaltung der Systemstrukturen, in denen personenbezogene Daten erhoben und verarbeitet werden, einer unzulässigen Datenverwendung vorzubeugen und die Selbstbestimmung der Nutzer sicherzustellen. Datenschutzrechtliche Probleme sollen von vorneherein durch eine Gestaltung der datenverarbeitenden Systeme vermieden werden.[57] Die bloß juristische Ausrichtung des Datenschutzes wird demgemäß durch die Technik korrigiert und die Technik gezielt zum Schutz der Privatsphäre genutzt.[58]

---

[55] Vgl. auch Post-Ortmann, RDV 1999, 102, 103.

[56] Vgl. hierzu die Ausführungen von Engel-Flechsig, DuD 1997, 8, 13, die er allerdings vor Novellierung des Teledienstedatenschutzgesetzes (TDDSG) zu § 4 TDDSG a.F. getätigt hat. In § 4 TDDSG a.F. war die nun in § 3a BDSG enthaltene Regelung des Systemdatenschutzes enthalten (siehe zur Novellierung des TDDSG insbesondere Fn. 27).

[57] So Sonntag, IT-Sicherheit kritischer Infrastrukturen, S. 170 mit dem Hinweis, dass dies einerseits durch Anonymisierung und Pseudonymisierung bewerkstelligt werden kann. Andererseits ist die Systemarchitektur entscheidend, durch die der Anfall von personenbezogenen Daten auf das absolut erforderlich Minimum reduziert und eine Akkumulation vermieden werden kann (durch Trennung von Verarbeitungsbereichen und Vermeidung von Funktionsbündelungen)..

[58] Siehe hierzu Bäumler in: Baeriswyl/Rudin, Perspektive des Datenschutzes, S. 354, der hier auch auf die Schlagworte „Datenschutz durch Technik“ und „datenschutzfreundliche Technik“ verweist. Siehe zu dem Bereich „Datenschutz durch Technik“ auch die Ausführungen von Pfitzmann in: v.Mutius/Bäumler, Datenschutzgesetze der dritten Generation, S. 18 ff., der in seinen Ausführungen hauptsächlich zur Datenvermeidung und Datensparsamkeit Stellung nimmt. Vgl. auch Weichert in: v.Mutius/Bäumler, Datenschutzgesetze der dritten Generation, S. 87, der darauf hinweist, dass Technik nicht nur Gefahren für Rechtsgüter eröffnet, sondern auch Instrumente zu deren Schutz entwickelt. Siehe außerdem Weichert, RDV 1999, 65 ff. Ebenso Stransfeld in: Schulte, Technische Innovation und Recht, S. 182, mit den Ausführungen, dass mit der Ausweitung telekommunikativer Aktivitäten die Zahl der potenziell einsichtnehmenden Akteure wachse, und erhöhtes Augenmerk auf die Realisierung technischer Optionen gerichtet werden müsse, die inhärent sicher sind, die also das Entstehen oder die

Dieses gerade dargestellte Prinzip der Datenvermeidung und Datensparsamkeit gemäß § 3a BDSG sowie das Prinzip des Datenschutzes durch Technik ist dem Systemdatenschutz zuzuordnen.[59] Entsprechend der Ausführungen zur Relevanz des Mehrpersonenverhältnisses ist Systemdatenschutz frühzeitig und bereits in der Planungsphase zu beachten.[60] So wird vertreten, dass insbesondere die Anbieter von Telekommunikationsdiensten gefordert sind, datenschutzfreundliche Produkte zu entwickeln und ihren Kunden anzubieten,[61] wobei sich der Grundsatz des Systemdatenschutzes jedoch grundsätzlich dadurch auszeichnet, dass er als übergreifende Regelung für alle Bereiche des Datenschutzrechts übernommen worden ist.[62]

Übermittlung personenbezogener Daten erst gar nicht erforderlich machen, wie etwa Verschlüsselung. Außerdem Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 108 mit dem Hinweis, dass es ein wesentliches Element des Rechts auf informationelle Selbstbestimmung ist, die zu einer Zweckerfüllung einer Aufgabe erforderliche Erhebung und Speicherung von Daten auf ein Minimum zu begrenzen. Siehe außerdem Enzmann/Scholz in: Roßnagel, Datenschutz beim Online-Einkauf, S. 84, die zunächst die Frage stellen, ob überhaupt Daten verarbeitet werden müssen und anschließend darauf verweisen, dass das Optimum der Datenvermeidung durch die Beschränkung auf die Verarbeitung anonymer oder pseudonymer Datensätze erreicht wird. BfD-Info 5, Datenschutz in der Telekommunikation, 2001, S. 77, nennt im Übrigen im Zusammenhang mit den datenschutzfreundlichen Technologien in der Telekommunikation § 3 Abs. 4 TDSV a.F. (TDSV vom 12.07.1996 (BGBl. I S. 982), nachfolgend: TDSV 1996) und der darin enthaltenen Verpflichtung, dass die Anbieter von Telekommunikationsdiensten sich an dem Ziel der Datenvermeidung und Datensparsamkeit auszurichten haben, welche sich nicht nur auf die technischen Anlagen beziehen, sondern auch auf die Datenverarbeitungsprozesse der Telekommunikation. Demnach seien Art und Umfang der Datenerhebung und –speicherung auf das für Telekommunikationszwecke erforderliche Maß zu beschränken. Vgl. auch Reinermann, Datenschutz im Internet – Internet im Datenschutz, S. 24 und dem Hinweis auf die „Datenschutztechnik“.

[59] Gola/Schomerus, BDSG, Einleitung Rn. 12. Siehe auch Hornung, MMR 2004, 3, 7 und Sonntag, IT-Sicherheit kritischer Infrastrukturen, S. 170, insbesondere auch dort Fn. 890.

[60] Siehe S. 7. Vgl. Koch, Internet-Recht, S. 895, der darauf verweist, dass Systemdatenschutz schon während des Software- und System-Engineering-Prozesses bei Gestaltung und Implementierung der späteren Systemstrukturen realisiert werden muss. Sollen beispielsweise personenbezogene Datenbestände von Mitarbeitern und Kunden im Internet zugänglich gemacht werden, müssen besondere Zugriffsabsicherungen implementiert werden.

[61] Siehe BfD-Info 5, Datenschutz in der Telekommunikation, 2001, S. 77. Siehe auch den Hinweis des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen, 14. Datenschutzbericht (1999), S. 9, dass der stetig zunehmende Einfluss der Telekommunikation auf das tägliche Leben den Einsatz datenschutzfreundlicher Technologien besonders dringend macht und darüber diskutiert werden muss, welche Techniken und Verfahren zur anonymen Nutzung, Datenvermeidung und Datenreduzierung in die Netz- und Geräteplanungen einbezogen werden können.

[62] Siehe hierzu Rasmussen, CR 2002, 36, 38, die darauf Bezug nimmt, dass durch die datenschutzfreundliche Gestaltung der Systeme die Selbstbestimmung der Nutzer sichergestellt werden soll.

Bei der Bedeutung dieses Themas ist besonders zu berücksichtigen, dass potenzielle Kunden aufgrund der vielfältigen Verknüpfungsmöglichkeiten[63] ihrer Daten im Internet sensibilisiert sind und vermehrt Augenmerk darauf legen werden, dass Systemdatenschutz beachtet wird. Daher sollte sich ein Diensteanbieter bereits aus wirtschaftlichem Eigeninteresse an diesem Ziel orientieren. Diese Selbstverpflichtung kann in der Vorstellung von Kunden ein besonderes Qualitätsmerkmal darstellen, um sich letztendlich für einen Diensteanbieter zu entscheiden.[64]

C. Gang der Untersuchung

Die nachfolgenden Ausführungen gliedern sich in vier Abschnitte.

Der erste inhaltliche Teil dieser Arbeit beinhaltet in Abschnitt 2 zunächst eine technische Einführung.
Hierbei ist es aufgrund der Komplexität und der vielfältigen technischen Details eines VPN nur möglich, einen Überblick und vereinfachte Darstellung über die bestehende und gängige Technik und deren Möglichkeiten zu geben, und zwar unter Berücksichtigung von aktuellen Produktbeschreibungen kommerzieller Anbieter und bestehender Literatur.

Der zweite Teil des Abschnitts 2 befasst sich mit den materiellen Grundlagen und Definitionen einer auf ein VPN bezogenen datenschutzrechtlichen Prüfung. Zunächst wird der Begriff des Online-Dienstes neu definiert. Weiterhin werden die Beteiligten eines VPN sowie die datenschutzrechtlichen Regelungen der §§ 91 ff. TKG, des TDDSG sowie des BDSG dargestellt, wobei ebenso die datenschutzrechtlichen Pflichten eines Diensteanbieters (Datenvermeidung, Unterrichtungspflichten und Sicherstellung technischer Schutzmaßnahmen sowie Verpflichtung zur Auskunftserteilung und Überwachung gegenüber staatlichen Behörden) behandelt werden.

[63] Siehe zu den vielfältigen Möglichkeiten zur Zusammenführung personenbezogener Daten im Internet im Besonderen auch Schaar, Datenschutz im Internet, Rn. 174.
[64] Vgl. auch Bizer in: Simitis, BDSG-Kommentar, § 3a BDSG Rn. 26, der ausführt, dass § 3a S. 2 BDSG die verantwortliche Stelle dazu verpflichtet, die Voraussetzungen für einen vom Betroffenen wahrzunehmenden Selbstdatenschutz zu treffen.

Im dritten Abschnitt dieser Arbeit wird der Datenschutz in Bezug auf einen *jeweiligen* Nutzers im Verhältnis zum *jeweiligen* Anbieter des VPN wie folgt untersucht:

1) Rechtliche Einordnung der Einzelleistungen eines VPN als Telekommunikationsdienst oder Teledienst im jeweiligen Personenverhältnis
2) Datenschutzrechtliche Prüfung und Prüfung der Pflichten eines jeweiligen Diensteanbieters (unter Berücksichtigung des im zweiten Abschnitt dargestellten Prüfungsschemas):
   - Datenvermeidung
   - Technische Schutzmaßnahmen
   - Schranken des Datenschutzes in Form von Auskunfts- und Überwachungsmaßnahmen

Der vierte Abschnitt befasst sich mit den datenschutzrechtlichen Interessen einer Person, die nicht selbst als aktiver Nutzer des VPN beteiligt ist. Daher steht nicht ein konkretes Dienstleistungsverhältnis im Vordergrund, sondern es sind die Rechte eines Betroffenen relevant, dessen Daten verarbeitet werden. Auch in diesem Zusammenhang steht das Mehrpersonenverhältnis und die Technik eines VPN im Vordergrund und es wird untersucht, inwieweit den im dritten Abschnitt dargestellten Anbietern und Nutzern des VPN datenschutzrechtliche Pflichten obliegen. Der Telearbeit kommt hierbei besondere Relevanz zu.

Im fünften Abschnitt werden die Ergebnisse zusammengefasst.

2. Abschnitt
Grundlagen der datenschutzrechtlichen Untersuchung

Grundlage der datenschutzrechtlichen Prüfung in dieser Arbeit sind technische Ausführungen zur Kommunikation im Internet und speziell im VPN (nachfolgend unter A.). Darüber hinaus werden ebenso die materiellen Grundlagen der rechtlichen Prüfung dargestellt (nachfolgend unter B.). Diese beinhalten die Darstellung der einschlägigen datenschutzrechtlichen bzw. datenschutzgesetzlichen Regelungen.

A. Technische Grundlagen

In den folgenden Abschnitten werden die technischen Grundlagen behandelt, die einem VPN zugrunde liegen. Sie verdeutlichen die technischen Möglichkeiten und die hieraus resultierenden Rechtsprobleme. Angesprochen werden allgemeine technische Grundlagen, wie der Aufbau einer Internetverbindung, technische Details von VPN sowie Funktionsprinzipien von E-Mail-Systemen.

I. Kommunikation im Internet

Kommunikation im Internet basiert auf unterschiedlichen Voraussetzungen und Regeln, wobei zunächst die Bedeutung von Protokollen und des OSI-Schichtenmodells im Rahmen einer Internetverbindung erläutert wird.

1. Internetverbindung

a. Protokoll

Um einen Dienst im Internet in Anspruch nehmen zu können, ruft der Rechner eines Nutzers (Client) einen anderen Rechner (Server) an (Client-Server-Prinzip).[65] Ein Protokoll stellt die Grundvoraussetzung dafür dar, dass diese Kommunikation realisiert werden kann. Es handelt sich um einen technischen

[65] Siehe Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I Rn. 56, der darauf hinweist, dass alle Internet-Dienste auf dem Client-Server-Prinzip beruhen.

Regelsatz, der die Datenübertragung zwischen den Rechnern sicherstellt. Ohne Verwendung von gleichen Protokolldaten wäre ansonsten keine Verständigung zwischen den Rechnern möglich.[66] Dies ist vergleichbar der menschlichen Sprache. Sofern zwei Personen miteinander kommunizieren möchten, müssen sie sich auf sprachliche Regeln einigen, die beide verstehen. So wie es unterschiedliche Sprachen gibt, gibt es unterschiedliche Protokolle. **Das Internet** als größtes öffentliches Netzwerk arbeitet mit dem Protokoll TCP/IP. Internet Protocol (IP) und Transmission Control Protocol (TCP) sind dafür verantwortlich, dass Daten über das Internet transportiert und zugestellt werden können bzw. Rechner miteinander kommunizieren können.[67] Die Datenübertragung im Internet basiert auf einer paketorientierten Übertragung. Das Internet-Protokoll (IP) ist dafür verantwortlich, dass die Datenpakete aufgespalten werden. Anders als bei einer Punkt-zu-Punkt-Verbindung (beispielsweise bei der Datenübertragung über die Telefonleitung) ist hier keine feststehende Verbindung notwendig. IP stellt einen verbindungslosen Dienst dar, ohne dass ein fester Pfad von Client zu dem Ziel erforderlich ist. [68] TCP (Transmission Control Protocol) hingegen ist für die fehlerfreie Übertragung der einzelnen Datenpakete zwischen den verschiedenen Rechnern bzw. Netzwerken verantwortlich, so dass diese am Zielort in der richtigen Reihenfolge sowie ohne Verluste wieder zusammengefügt werden können.[69] Für den Aufbau einer Internetverbindung ist regelmäßig noch ein weiteres Protokoll von Bedeutung, da der Anschluss eines Rechners „an das Internet“ überwiegend als physikalische Verbindung über das Telefonnetz erfolgt.[70]

---

[66] Hobert, Datenschutz und Datensicherheit im Internet, S. 45; Eichhorn, Internet-Recht, S. 27; Schneider, MMR 1999, 571, 572.

[67] Schaar, Datenschutz im Internet, Rn. 22; Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 24; Hobert, Datenschutz und Datensicherheit im Internet, S. 37; Eichhorn, Internet-Recht, S. 225; Sieber in: Hoeren/Sieber, Teil 1 Rn. 42 ff.; Cichon, Internetverträge, Rn. 15; teia (Hrsg.), Recht im Internet, S. 16 ff.; Dilger, Verbraucherschutz bei Vertragsabschlüssen im Internet, S. 9; Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I, Rn. 47; Martens/Schwarz-Gondek in: Bräutigam/Leupold, Glossar S. 1090/1091; Glatt, Vertragsschluss im Internet, S. 20; Wildemann, Vertragsschluß im Netz, S. 3; Schneider, MMR 1999, 571, 571; Kröger/Göers/Hanken, Internet für Juristen, S. 483.

[68] Davis, IPSec, S. 22. TCP (Transmission Control Protocol) hingegen ist für die fehlerfreie Übertragung der einzelnen Datenpakete zwischen den verschiedenen Rechnern bzw. Netzwerken verantwortlich, so dass diese am Zielort in der richtigen Reihenfolge sowie ohne Verluste wieder zusammengefügt werden können..

[69] Voss, Das große PC & Internet Lexikon 2007, „TCP/IP“ S. 789; Sieber in Hoeren/Sieber, Teil 1 Rn. 45 ff. Die einzelnen Datenpakete verfügen nicht nur über den Inhalt der Nachricht, sondern auch über einen so genannten Header (Kopf), der die Adressen von Sender und Empfänger beinhaltet

[70] Siehe hierzu die folgenden Ausführungen auf S. 25.

Eine Datenübertragung **über die Telefonleitung** erfolgt über das Point-to-Point-Protokoll (PPP). PPP ermöglicht eine Verbindung über leitungsvermittelte Netze oder Festverbindungen,[71] wobei Point-to-Point (Punkt-zu-Punkt) bedeutet, dass zwei fixe Stellen für den Verbindungsaufbau existieren müssen. Das Merkmal der Leitungsvermittlung besteht darin, dass für die gesamte Dauer der Verbindung eine permanente Reservierung von Kanälen (Bandbreiten) zwischen den beiden Punkten (Sender und Empfänger) aufrechterhalten wird.[72]
Diese Verbindung ist den Kommunikationspartnern fest zugewiesen und bleibt auch bestehen, wenn sie in Kommunikationspausen nicht benötigt wird. Telefonnetze (z.B. die ISDN-Technologie) arbeiten nach diesem Vermittlungsverfahren.[73]

b. Internet-Protokoll-Adressen

Eine Internet-Protokoll-Adresse (IP-Adresse) wird von jedem Rechner im Internet benötigt, um angesprochen und identifiziert werden zu können. Jede komplette IP-Adresse ist eine 32-Bit-Zahl, die sich wiederum aus vier 8-Bit-Zahlen (Oktetts) zusammensetzt.
Normalerweise wird die Adresse als 4-Byte-Dezimalzahl von 0 bis 255 durch je einen Punkt getrennt dargestellt (z.B. 191.255.255.255).[74]
Generell kann zwischen statischen und dynamischen IP-Adressen unterschieden werden.

---

[71] Lipp, VPN, S. 277.
[72] Zum Begriff „Bandbreite“ siehe auch Schneider, Lexikon der Informatik und Datenverarbeitung, S. 80.
[73] Vgl. hierzu Böhmer, Virtual Private Networks (2. Auflage), S. 18 Fn. 2. Die Einführung der modernen Kommunikations- und Übertragungstechnologien, wie ISDN, war Folge der technologischen Entwicklung der Veränderung bei Netzen und Endgeräten. Die Einführung digitaler, transparenter und von hochentwickelten Computern gesteuerter Netze hat dazu geführt, dass viele der zuvor netzinternen Funktionen (die nur von dem entsprechenden Netzbetreiber wahrgenommen werden konnten) mehr und mehr auch außerhalb des Netzes und von den immer höher entwickelten Endgeräten übernommen werden können (siehe auch Grünbuch über die Entwicklung des Gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte, KOM (87) 290 endg. vom 30.06.1987).
[74] Siehe zur IP-Adresse anstatt vieler etwa: Kröger, Rechtsdatenbanken, S. 410; Köhntopp/Köhntopp, CR 2000, 248, 248; Martens/Schwarz-Gondek in: Bräutigam/Leupold, Glossar S. 1079; Glatt, Vertragsschluss im Internet, S. 20/21; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 49; Hobert; Datenschutz und Datensicherheit im Internet, S. 225; Göckel in: Königshofen, Das neue Telekommunikationsrecht in der Praxis, S. 127 ff.

Statische IP-Adresse bedeutet, dass ein Kunde stets die gleiche Adresse bei den Internetvorgängen nutzt, während bei dynamischen IP-Adressen die Zuweisung einer temporären IP-Adresse für jede einzelne Internetsitzung erfolgt.[75] Letzteres ist im Rahmen von Einwahlvorgängen der Regelfall. Dies beruht darauf, dass IP-Adressen knapp sind und Anbieter diese nicht fest an ihre Kunden vergeben, sondern lediglich zu den Zeitpunkten zuweisen, zu welchen eine Internetsitzung erfolgen soll.[76]

c. OSI-Schichtenmodell

Zur Beschreibung eines Kommunikationsvorganges zwischen Rechnern im Internet wurde ein Modell entwickelt, das so genannte OSI-Schichtenmodell.[77] Die Arbeitsgruppe OSI (Open Systems Interconnection) wurde 1977 durch die International Standard Organisation (ISO) zur Erarbeitung allgemeiner Standards für offene Kommunikationssysteme ins Leben gerufen.
Offene Systeme sind in sich abgegrenzte Systeme, die mit anderen Systemen in Form eines Nachrichtenaustausches kommunizieren möchten.[78] Dieses OSI-Schichtenmodell legt die Funktionen und Prinzipien der Datenübertragung zwischen den einzelnen Systemen fest, wobei die Kommunikationsfunktionen in sieben Schichten eingeteilt werden, die bei einem Kommunikationsvorgang jeweils miteinander in Verbindung treten.[79]

Diese sieben Schichten lassen sich wiederum grob in zwei Abschnitte untergliedern:

- den Abschnitt der Transportprotokolle
- und den der Anwendungsprotokolle.[80]

---

[75] Köhntopp/Köhntopp, CR 2000, 248, 248; Geis, Recht im eCommerce, S. 144/145; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 41/42; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 92/93/94; Kloepfer, Informationsrecht, § 11 Rn. 172; Schaar, Datenschutz im Internet, Rn. 169 ff.
[76] Köhntopp/Köhntopp, CR 2000, 248, 248; Koenig/Neumann, K&R 1999, 145, 148 Fn. 35.
[77] Siehe zum OSI-Schichtenmodell auch Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 99 ff.; Tanenbaum, Computernetzwerke, S. 54 ff.
[78] Böhmer, Virtual Private Networks (2. Auflage), S. 20/21.
[79] Böhmer, Virtual Private Networks (2. Auflage), S. 22; Pankoke, Von der Presse- zur Providerhaftung, S. 41 ff.; Voss, Das große PC & Internet Lexikon 2007, „OSI-Schichtenmodell S. 592.
[80] Böhmer, Virtual Private Networks (2. Auflage), S. 22.

Die Schichten 1-4 (Physical Layer, Data-Link Layer, Network Layer, Transport Layer) bilden die Transportfunktionen. Zu den Transportprotokollen zählt etwa TCP/IP.

Die Schichten 5-7 (Session Layer, Presentation Layer, Application Layer) beschreiben die Anwendungsprotokolle.[81]

Anwendunggschicht/Application Layer
Darstellungsschicht/Presentation Layer
Sitzungsschicht/Session Layer
Transportschicht/Transport Layer
Vermittlungsschicht/Network Layer
Sicherungsschicht/Data-Link Layer
Bitübertragungsschicht/Physical Layer

OSI-Referenzmodell

Die Anwendungsprotokolle stellen Dienste zur Verfügung, um Daten auf dem Rechner darstellen zu können. So gehören beispielsweise ftp (file transfer protocol),[82] smtp (simple mail transfer protocol)[83] oder http (hyper text transfer protocol)[84] der Anwendungsschicht an.

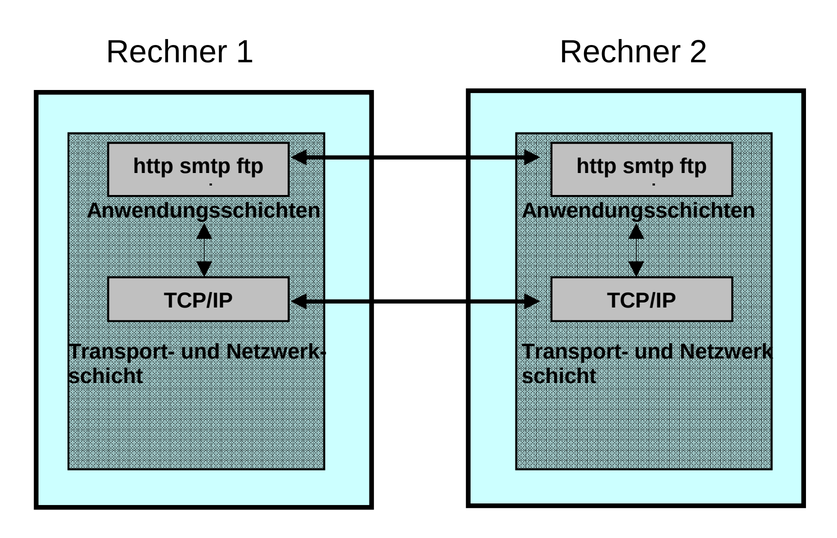
[81] Böhmer, Virtual Private Networks (2. Auflage), S. 23.

[82] ftp ist beispielsweise im Zusammenhang mit dem Universitätsbetrieb bekannt. Viele Universitäten stellen ihren Angehörigen ftp-Zugänge bereit, damit diese Daten auf den Universitätsrechnern einsehen und abrufen können. Bei ftp handelt es sich um ein Übertragungsprotokoll, wobei der Begriff „Übertragungsprotokoll“ speziell bei der Datenfernübertragung verwendet wird. Seine Aufgabe besteht darin, eine fehlerfreie Übertragung der Informationen zu gewährleisten, Fehler in der Übertragung zu erkennen und zu korrigieren. ftp wird eingesetzt bei Netzen, die TCP/IP als Netzwerkprotokoll nutzen, wie etwa das Internet; vgl. Schaar, Datenschutz im Internet, Rn. 15; Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 85; Hobert, Datenschutz und Datensicherheit im Internet, S. 43; Eichhorn, Internet-Recht, S. 26; Kröger/Kuner, Internet für Juristen, S. 11; Martens/Schwarz-Gondek in: Bräutigam/Leupold, Glossar S. 1075; Geis, Recht im eCommerce, Glossar S. 203; Ritz, Inhalteverantwortlichkeit von Online-Diensten, S. 26; Schneider, MMR 1999, 571, 572.

[83] Der Absender einer E-Mail benutzt regelmäßig das simple mail transfer protocol (smtp), um seine E-Mails versenden zu können. Siehe hierzu auch Schaar, Datenschutz im Internet, Rn. 12; Sieber in: Hoeren/Sieber, Teil 1 Rn. 114 ff.; Cichon, Internetverträge, Rn. 28; teia (Hrsg.), Recht im Internet, S. 34 ff.; Hobert, Datenschutz und Datensicherheit im Internet, S. 40.

[84] Cichon, Internetverträge, Rn. 26; Lipp, VPN, S. 78; Campo/Pohlmann, Virtual Private Networks, S. 350; Davis, IPSec, S. 43. Websites sind in der Seitenbeschreibungssprache html (hyper text markup language) geschrieben, die die Darstellung der Informationen und Bilder dieser Websites ermöglicht. Wird diese Website von einem Nutzer aufgerufen, veranlasst das Übertragungsprotokoll „http“, dass die einzelnen Seiten auf dessen Bildschirm erscheinen.

Zur Vereinfachung kann man sich vorstellen, dass es sich bei den Schichten um mehrere einzelne Module handelt, von denen jedes einzelne Modul während der Kommunikation und als Voraussetzung der Kommunikation eine andere Aufgabe zu erfüllen hat.[85]



TCP/IP gehört der Transportschicht an. Bei ftp, http, smtp handelt es sich um Anwendungsprotokolle, die auf diese Transportschicht aufsetzen, um die Daten zu übertragen.[86] Jede Schicht kommuniziert nur mit ihrer entsprechenden (Rechner-)Schicht auf der Gegenseite.

Diese jeweiligen Schichten des OSI-Schichtenmodells, die hier gemäß der obigen Ausführung zur Vereinfachung in zwei Abschnitte gegliedert worden sind, bedingen sich gegenseitig, indem die in einer Schicht angesiedelten Dienste nur auf Dienste zugreifen können, die durch die darunter liegenden Schichten angeboten werden. Umgekehrt stellen die unteren Schichten wiederum Dienste für die Funktionen in der übergeordneten Schicht bereit. TCP/IP als ein für die Datenübertragung und Paketaufspaltung verantwortliches Protokoll[87] wird also stets im Internet als notwendige Transportschicht für die Übertragung benötigt.

[85] Campo/Pohlmann, Virtual Private Networks, S. 330.
[86] Davis, IPSec, S. 43.
[87] Siehe S. 20.

2. Infrastruktur

a. Telekommunikationsnetze

Aufgrund dessen, dass „das Internet" eine Verknüpfung einer Vielzahl von (Rechner-) Netzen darstellt,[88] wird die Beschreibung der Infrastruktur in dieser Arbeit so vereinfacht dargestellt, wie es für die anschließende juristische Diskussion erforderlich ist.

Der Anschluss eines Rechners eines Nutzers an das Internet erfolgt zumindest in Deutschland[89] überwiegend als physikalische Verbindung über das Telefonnetz bzw. über die Teilnehmeranschlussleitung von so genannten Carriern,[90] wie beispielsweise der Deutschen Telekom AG.[91]

---

[88] Zum Zusammenschluss der Netze zum weltumspannenden Internet vgl. anstatt vieler anderer Cichon, Internetverträge, Rn. 11 ff.; Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I Rn. 46, Schneider, MMR 1999, 571, 571; Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 10.

[89] Siehe zu den Gründen, dass sich die Prüfung in dieser Arbeit lediglich auf die Datenverarbeitung in Deutschland konzentrieren soll, S. 87 ff.

[90] Vgl. Summa: in Holznagel/Nelles/Sokol, TKÜV, S. 24, der für die Anbieter, die die Leitungen bereitstellen bzw. eigene Netze betreiben den Begriff „Carrier" verwendet (Deutsche Telekom AG, arcor, NetCologne). Vgl. zum Begriff „Carrier" auch Schaar, Datenschutz im Internet, Rn. 21. Siehe auch Kath/Riechert, Internet-Vertragsrecht, Rn. 46 ff.; Schneider, Verträge über Internet-Access, S. 95, die beispielhaft auf NetCologne und Hansenet und deren Funktion auf Stadtebene verweist).

[91] Der Zugang in das Internet bzw. die Verbindung/Vernetzung mit anderen (Computer-) Netzwerken mittels des Telefonkabels, welches meist aus Kupferkabel (Kupferdoppelader), in wenigen Fällen aus Glasfaser besteht (vgl. Kath/Riechert, Internet-Vertragsrecht, Rn. 47), stellt zur Zeit die am meisten genutzte Methode für den Internetzugang dar. So bestehen zwar weitere Anbindungsmöglichkeiten an das Internet, etwa über Fernsehkabel, Funk (Wireless Technologien), Stromnetz oder Satellit. Bei der so genannten WLL (Wireless Local Loop)-Technik ist jedoch ergänzend darzulegen, dass es sich hierbei lediglich um ein lokales Funknetz handelt (Siehe zur W-Lan-Technik ebenso Zimmer, CR 2003, 893 ff.). Hierzu werden für ein bestimmtes, lokal begrenztes Gebiet (Büroraum) zentrale Funkknoten eingesetzt, die die Versorgung der Clients mit der drahtlosen Netzanbindung übernehmen (siehe auch Frankfurter Allgemeine Zeitung vom 23. Februar 2004, S. 17 zur Überbrückung kurzer Distanzen und dem Funkstandard „Bluetooth"). Bei W-Lan wird also nur ein Teil der „Wegstrecke", nämlich vom Rechner zur Telefonanschlussdose per Wireless Local Loop überbrückt wird, so dass die anschließende Datenweiterleitung wiederum über das Telefonnetz erfolgt. Die Weiterentwicklung der W-Lan-Technik „Wimax" zur Überbrückung der „letzten Meile" und damit von Entfernungen bis zu 50 km im Umkreis eines Senders ist noch nicht flächendeckend ausgereift (siehe Frankfurter Allgemeine Zeitung vom 23. Februar 2004, S. 17; vgl. hierzu auch die an die Regulierungsbehörde für Post und Telekommunikation (Bundesnetzagentur) übersandte Stellungnahme der BT (Germany) GmbH & Co. oHG vom 09.01.2004, S. 5, abrufbar unter http://www.bundesnetzagentur.de/media/archive/520.pdf (Website vom 30.09.2006). Letzteres gilt ebenso für die Anbindung mittels Fernsehkabel, was sich auch nach dem Verkauf des restlichen Kabelnetzes der Deutschen Telekom AG an die Finanzinvestoren Goldman Sachs Capital, Apax Partners und Providence Equity vorerst nicht wesentlich ändern wird (siehe Frankfurter Allgemeine Zeitung vom 14. März 2003, S. 24 sowie die an die Regulierungsbehörde für Post und Telekommunikation (Bundesnetzagentur) übersandte Stellungnahme der BT (Germany) GmbH & Co. oHG vom 09.01.2004, S. 4, abrufbar unter http://www.bundesnetzagentur.de/media/archive/520.pdf (Website vom 30.09.2006). Die Satellitentechnik weist keine Rückkanalfähigkeit auf und bedeutet, dass Daten zwar aus dem

Die Teilnehmeranschlussleitung, die unter dem Begriff „letzte Meile“ besser bekannt sein dürfte, führt zu einem Hauptverteiler (HVT), einer Vermittlungsstelle, der Deutschen Telekom AG.[92] An diesem Ort kann die Deutsche Telekom AG auch anderen Carriern einen eigenen Kollokationsraum (einen räumlichen Zugangsbereich) zur Verfügung stellen und die Teilnehmeranschlussleitung zum eigenen Betrieb „übergeben“.[93] Die Deutsche Telekom AG hat über Deutschland verteilt an mehreren Standorten im Teilnehmeranschlussbereich technische Einrichtungen, Hauptverteiler (HVT), platziert, in denen die einzelnen Teilnehmeranschlussleitungen eines geographischen Einzugsbereichs zusammenlaufen. Dort wird für die Umschaltung gesorgt, um ankommende Daten in andere, weltweite Netze weiterzuleiten.

Internet herunter geladen (Download) werden können, für das Versenden von Daten wird allerdings zusätzlich noch das Telefonkabel bzw. eine ISDN-Verbindung benötigt (vgl. zu den hohen Kosten eines Multimedia-Satellitensystems auch die an die Regulierungsbehörde für Post und Telekommunikation (Bundesnetzagentur übersandte Stellungnahme der BT (Germany) GmbH & Co. oHG vom 09.01.2004, S. 5, abrufbar unter http://www.bundesnetzagentur.de/media/archive/520.pdf (Website vom 30.09.2006). Die Internetanbindung über das Stromnetz ist in technischer Hinsicht noch nicht ausgereift ist und unterliegt daher einer gewissen Störanfälligkeit.

[92] Siehe zum Begriff der Vermittlungsstelle Voss, Das große PC & Internet Lexikon (1. Auflage), S. 919 (in der aktuellen Auflage „2007“ (S. 800) erläutert Voss den Begriff der Vermittlungsstelle lediglich im Hinblick auf T-Net).

[93] Wer Übertragungswege, welche die Grenze eines Grundstückes überschreiten, betreiben möchte, benötigte von der Bundesnetzagentur gemäß § 6 TKG a.F. eine Lizenz. Nach der Novellierung des TKG besteht nunmehr eine Meldepflicht bei der RegTP gemäß § 6 TKG (n.F.). Die Lizenzierungspflicht sollte bzw. die Meldepflicht soll gewährleisten, dass diejenigen Dienste im Bereich der Telekommunikation, die für die Grundversorgung der Bevölkerung von erheblicher Bedeutung sind, nur von solchen Unternehmen erbracht werden, die dafür zumindest die allgemeinen gewerberechtlichen Voraussetzungen erfüllen (vgl. Schütz in: TKG-Kommentar (2. Auflage), § 6 TKG Rn. 3; siehe Zimmer, CR 2003, 893, 894 ff. zur Abschaffung der Lizenzpflicht, mit der ebenso verbunden ist, dass es nunmehr nicht mehr darauf ankommt, ob bei dem Betrieb von Übertragungswegen Grundstücksgrenzen überschritten werden. Vgl. zum Überschreiten einer Grundstücksgrenze nach dem grundbuchrechtlichen Grundstücksbegriff Manssen: in Manssen, Kommentar Telekommunikations- und Multimediarecht, § 6 TKG(1998), Band 1, Rn. 3. Zur ersatzlosen Streichung der Lizenzpflicht gemäß § 6 TKG a.F. siehe Schütz in TKG-Kommentar (3. Auflage), § 6 TKG Rn. 1 sowie Lammich in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 6 TKG(2004), Band 2, Rn. 2). Die Anfänge dieser Liberalisierung finden eine entscheidende Grundlage in der Richtlinie 90/388/EWG der Kommission vom 28.06.1990 über den Wettbewerb auf dem Markt für Telekommunikationsdienste (90/388/EWG vom 28.6.1990, ABl. Nr. L 192 vom 24.07.1990, S. 10; geändert durch 94/46/EG, ABl. Nr. L 268 vom 19.10.1994, S. 15; geändert durch 95/51/EG, ABl. Nr. L 256 vom 26.10.1995, S. 49; geändert durch 96/2/EG, ABl. Nr. L 20 vom 26.01.1996, S. 59; geändert durch 96/19/EG, ABl. Nr. L 74 vom 22.03.1996, S. 13 = Diensterichtlinie). Nach Artikel 2 dieser Richtlinie mussten die Mitgliedstaaten die Beseitigung der besonderen oder ausschließlichen Rechte bei der Erbringung von Telekommunikationsdiensten mit Ausnahme des Sprach-Telefondienstes gewährleisten. Sie hatten darüber hinaus sämtliche erforderlichen Maßnahmen zu ergreifen, um allen interessierten Betreibern das Recht auf Erbringung von Telekommunikationsdiensten zu ermöglichen.

Diese Vermittlungsstelle ist im Übrigen notwendiger Konzentrationspunkt für eine anschließende Datenfernübertragung, da von diesem Punkt aus eine Datenweiterleitung in andere Netze erfolgt.

Sofern ein Anbieter über eigens von ihm administrierte Leitungen verfügt,[94] die

---

[94] Das Recht eines privaten Anbieters, einen Internetzugang über eigene Netze anzubieten, ist der Liberalisierung auf dem gesamten europäischen Telekommunikationsmarkt zu verdanken. Siehe hierzu die Ausführungen von Kirsten in: Hoeren/Sieber, Teil 10 Rn. 25. Staatliche Monopole im deutschen Telekommunikationssektor reichen im Übrigen bis in das 19. Jahrhundert zurück. So legte § 1 des Telegraphengesetz von 1892 (Gesetz über das Telegraphenwesen des Deutschen Reichs, 6.4.1892, RGBl. S. 467 ff.) fest, dass das Recht, Telegraphenanlagen für die Vermittlung von Nachrichten zu errichten und zu betreiben, ausschließlich dem Reich bzw. den Ländern Württemberg und Bayern, welche eigene Postverwaltungen hatten (§ 15 des Telegraphengesetzes), zusteht. An der staatlichen Zuständigkeit änderte auch das Fernmeldeanlagengesetz (FAG) nichts, welches als Neubekanntmachung des geänderten Telegraphengesetzes im Januar 1928 trat in Kraft trat (Fernmeldeanlagengesetz vom 14.01.1928, RGBl. I S. 8; Artikel III des Gesetzes zur Änderung des Telegraphengesetzes vom 03.12.1927, RGBl. I S. 331 ff.; siehe Simon, ArchivPT 1996, 142, 144 zum Netzmonopol der Deutschen Telekom AG nach § 1 Abs. 2 FAG). Europarechtliche Harmonisierungsvorgaben haben letztendlich den Weg für eine Öffnung des Zugangs zu den öffentlichen Telekommunikationsnetzen geebnet (Richtlinie für den offenen Netzzugang RL 90/387/EWG, ABl. Nr. L 192 vom 24.07.1990, S.1, ONP-Rahmenrichtlinie). So nahm die europäische Telekommunikationspolitik ihren Anfang im Jahr 1987 mit einem Grünbuch zur Liberalisierung des Telekommunikationsmarktes (Grünbuch über die Entwicklung des Gemeinsamen Marktes für Telekommunikationsdienst(-leistung)en und Telekommunikationsgeräte, KOM (87)290 endg. vom 30.06.1987). Mit dieser Politik wurden drei Hauptziele verfolgt, die in der Liberalisierung der monopolisierten Marktsegmente, der Harmonisierung des europäischen Telekommunikationssektors mit Hilfe gemeinsamer Regeln und Normen sowie der strikten Anwendung der Wettbewerbsregeln auf die liberalisierten Marktsegmente, um heimliche Absprachen sowie den Missbrauch oder die Schaffung dominanter Marktstellungen zu verhindern, bestanden. Aufgrund der Entmonopolisierungsabsicht dieser Telekommunikationspolitik, welche in dem Telekommunikationsgesetz vom 25. Juli 1996 (Telekommunikationsgesetz vom 25. Juli 1996, BGBl. I S. 1120) seine Umsetzung fand, ist es seitdem ebenfalls privaten Diensteanbietern möglich, Nutzern Übertragungswege bereit zu stellen bzw. über eigens administrierte Telefonanschlussleitungen den Zugang in das Internet zu verschaffen. Bis zur durch die Aufhebung des Sprachtelefondienstmonopols bedingten vollständigen Liberalisierung der Telekommunikationsmärkte zum 01.01.1998 (vgl. § 97 Abs. 2 TKG a.F., § 99 Abs. 1 Nr. 1 lit. b TKG a.F.) war allerdings die Deutsche Bundespost bzw. deren Nachfolgerin die Deutsche Telekom Monopolist im Telekommunikationssektor und einzig und allein zur Bereitstellung von Netzen berechtigt. Die Gründung der Deutschen Telekom ist auf die Postreformen I und II zurückzuführen, in deren Rahmen die "bundeseigene Postverwaltung" neu strukturiert wurde. Das Poststrukturgesetz vom 8. Juni 1989 (BGBl. I S. 1026) gliederte das Sondervermögen Deutsche Bundespost in drei teilrechtsfähige "öffentliche Unternehmen" (§§ 1, 2, 5 des Gesetzes über die Unternehmensverfassung der Deutschen Bundespost - Postverfassungsgesetz - = Artikel 1 des Poststrukturgesetzes (Postreform I)), wovon ein Unternehmen, neben Postbank und Postdienst, die Telekom war. Gemäß § 1 des Gesetzes zur Umwandlung der Unternehmen der Deutschen Bundespost in die Rechtsform der Aktiengesellschaft (Postumwandlungsgesetz (PostUmwG) = Artikel 3 des Gesetzes zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz) vom 14. September 1994 (BGBl. I S. 2325; in Kraft getreten gemäß Artikel 15 am 01.01.1995) wurden die drei Unternehmen in Aktiengesellschaften umgewandelt (Postreform II); das Teilsondervermögen wurde auf diese Aktiengesellschaften übertragen (§ 2 Abs. 1 PostUmwG). Siehe zur Postreform I auch die Ausführungen bei Statz in: Königshofen, Das neue Telekommunikationsrecht in der Praxis, S. 65 ff. Seit Bekanntmachung des Telekommunikationsgesetzes im Jahre 1996 hängt dieses Recht für private Anbieter bzw. Provider lediglich von der Vergabe einer Lizenz seitens der Regulierungsbehörde für Post und

als regionales oder überregionales Transportnetz miteinander verbunden sind,[95] wird diese Infrastruktur als Backbone bezeichnet.[96] Diese Backbone-Netze sind in der Regel redundant ausgelegt, was bedeutet, dass bei Ausfall einer Leitung eine andere Leitung für die Datenübertragung sorgt.[97] Große Unternehmen sind oft unmittelbar mit dem Backbone eines Anbieters verbunden.[98]

Darüber hinaus gibt es größere Betreiber, die internationale Backbones betreiben.[99] Der Backbone eines Providers übernimmt die Datenweiterleitung in andere Netze oder Backbones, wobei eine Datenübermittlung zwischen Backbones oder in das Netz eines anderen Anbieters über so genannte Peering-Points stattfindet.[100]

Telekommunikation (RegTP) bzw. (nach neuem Recht des TKG) von einer Meldepflicht ab (vgl. Fn. 93).

[95] Siehe Summa in: Holznagel/Nelles/Sokol, TKÜV, S. 25.

[96] Siehe zur Vertragsstruktur der Internet-Backbone-Betreiber auch die Ausführungen bei Petri/Göckel, CR 2002, 329 ff., dort zum Begriff „redundant" insbesondere auch S. 330 Fn. 14. Backbones zeichnen sich dadurch aus, dass sie regelmäßig höhere Bandbreiten zulassen, und damit für den Nutzer den Vorteil der besseren Datenübertragung bieten (vgl. auch Petri/Göckel, CR 2002, 329, 330, die darauf verweisen, dass heutzutage Geschwindigkeiten bis 30 Gbit/s im Kernbereich eines Backbones möglich sind). Siehe außerdem zu den vertraglichen Backbone-Klauseln Spindler in: Spindler, Vertragsrecht der Internet Provider, Teil IV Rn. 107 ff.

[97] Vgl. die Ausführungen sowie das Schema bei Petri/Göckel, CR 2002, 329, 330, die darstellen, dass sich die Einrichtungen des Anbieters innerhalb des jeweiligen PoPs befinden, um den Anschluss an das eigene Backbone zu realisieren.

[98] Tanenbaum, Computernetzwerke, S. 77.

[99] Tanenbaum, Computernetzwerke, S. 77.

[100] Peering-Points sind Übergabepunkte zu anderen Netzen bzw. Netzwerken. Vgl. auch Petri/Göckel, CR 2002, 418 ff., die darauf hinweisen, dass es keine klare Definition für den Begriff „Peering" gibt, auch nicht in den so genannten Requests for Comments der „Internet Engineering Task Force" („IETF", zu deutsch: Internet-Entwickler-Einsatzgruppe. Die IETF verbreitet regelmäßig Vorschläge und Informationen in Form von RFCs (Request for Comments), siehe zur IETF außerdem S. 35 Fn. 145. Siehe zu RFC die Ausführungen bei Voss, Das große PC & Internet Lexikon 2007, „RFC"S. 695, der darlegt, dass unter RFCs die Dokumente bzw. Vorschläge zur technischen Standardisierung des Internets verstanden werden. Diese können beispielsweise von Firmen oder Organisationen eingereicht werden und sind rechtlich nicht bindend). Überwiegend wird jedoch unter Peering die Zusammenschaltungen von öffentlichen Netzen im Internet ohne gegenseitige Verrechnung des verursachten Verkehrs verstanden (Petri/Göckel, CR 2002, 418, 418). Siehe Tanenbaum, Computernetzwerke, S. 73/77 zur Zusammenschaltung der größeren Backbones über so genannte NAPs (Network Access Points), einem lokalen Raum, in dem mehrere Router verschiedener Backbone-Betreiber zur Datenweiterleitung miteinander verbunden sind.

b. Internetzugangsknoten (Access-Providing)

Für die Datenfernübertragung im Netzverbund des Internets müssen darüber hinaus in den entsprechenden Datenfernübertragungsleitungen, die an die Vermittlungsstelle angeschlossen sind, Internetzugangsknoten vorhanden sein. An diese Internetzugangsknoten, auch PoPs (Point of Presence) genannt , sind wiederum Netze angeschlossen.[101] Regelmäßig hat der Nutzer bzw. Client eine Software auf seinem Rechner installiert und kann sich mittels eines Passwortes in das Internet bzw. den Internetzugangsknoten des Anbieters einwählen.[102]

Bei jeder Einwahl, unabhängig ob per Modem, ISDN[103] oder DSL[104] in das Internet erfolgt die Zuweisung der dynamischen IP-Adresse[105] mittels eines DHCP-Servers (Dynamic Host Configuration Protocol), wobei sich die DHCP-Funktion auf dem Internetzugangsknoten bzw. PoP oder der dem nachgelagerten RADIUS-Server befindet.[106]
Auf dem RADIUS-Server können Passwörter, Parameter und Rechte aller Nutzer zentral festgelegt und verwaltet werden.[107]
Bei DSL und einer Flatrate wird eine dynamische IP-Adresse für einen längeren Zeitraum zugewiesen.[108]
Die Verbindung ins Internet über das Telefonnetz kann außerdem als sogenannte Standleitung ausgestaltet sein. Dies bedeutet, dass der jeweilige Teilnehmer über die Telefonleitung eine permanente Verbindung zu einem Internetzugangsknoten (im Backbone) eines Anbieters hat, ohne sich erneut

[101] Vgl. Summa in: Holznagel/Nelles/Sokol, TKÜV, S. 26.
[102] Vgl. auch Kröger/Kuner, Internet für Juristen, S. 6.
[103] ISDN ist die Abkürzung für „Integrated Services Digital Network“ und bezeichnet ein öffentliches Digitalnetz für Daten, Sprache und Bild, siehe auch die Definition bei Kröger, Rechtsdatenbanken, S. 410.
[104] Im Rahmen von DSL (Digital Subscriber Line) wird ebenso die Telefonleitung genutzt, die allerdings mittels eines speziellen DSL-Modems in drei Kanäle unterteilt wird (vgl. zu DSL Voss, Das große PC & Internet Lexikon 2007, S. 256 ff.). Siehe zu DSL ebenso Tanenbaum, Computerarchitektur, S. 136 mit dem Hinweis, dass es sich bei DSL mehr um ein Marketingkonzept als um ein besonderes technisches Konzept handelt.
[105] Zur IP-Adresse siehe oben S. 21.
[106] Siehe zu DHCP auch Voss, Das große PC & Internet Lexikon 2007, S. 222.
[107] Buckbesch/Köhler, Virtuelle Private Netze, S. 104; Böhmer, Virtual Private Networks (2. Auflage), S. 245.
[108] Zum Begriff der Flatrate siehe Kroiß/Schuhbeck, Jura Online, S. 7. Siehe auch die obigen Ausführungen zu DSL auf S. 29.

einwählen zu müssen.[109] In diesem Falle ist ihm eine feste IP-Adresse zugewiesen.[110]

Von dieser Standleitung ist die gerade angesprochene DSL-Technik abzugrenzen. Auch wenn der Nutzer den Eindruck hat, er wäre im Rahmen von DSL ständig mit dem Internet verbunden, ist dennoch nach 15 Minuten, spätestens 24 Stunden, eine erneute Einwahl in einen Internetzugangsknoten erforderlich, sofern innerhalb dieser Zeit keine Daten übertragen worden sind, und der Anbieter daher eine Trennung vom Netz vorgenommen hat.[111]

c. DNS-Server

Aufgrund der schwer zu merkenden Ziffernkombination der IP-Adressen ist ein System entwickelt worden,[112] um IP-Adressen in lesbare Namen (Domains) umzuwandeln, das so genannte Domain Name System (DNS).[113]

Der Client bzw. einzelne Nutzer kann dementsprechend anstatt der IP-Adresse einen Domain-Namen, wie beispielsweise www.Anbieter-X.de, in seinen Browser[114] eingeben.[115] Die Eingabe der Domain-Namen in den Browser kann allerdings nur dann funktionieren, sofern die Zuordnung zwischen Domain-Namen und IP-Adresse irgendwo festgehalten worden ist. Diesen Zweck erfüllen die Domain-Name-Server.

Der Anbieter, der seinen Kunden den Internetzugang anbietet, verfügt in aller Regel über einen Domain-Name-Server, bei welchem die Informationen

[109] Vgl. Piepenbrock in: TKG-Kommentar (2. Auflage), Glossar S. 1579 zur Begriffsdefinition der „Festverbindung“ und der synonymen Begriffe „Standleitung“ und „Mietleitung“ (in der dritten Auflage des Beck´schen TKG-Kommentars ist kein Glossar enthalten, so dass hier auf die zweite Auflage verwiesen wird).

[110] Siehe auch die an die Regulierungsbehörde für Post und Telekommunikation (Bundesnetzagentur) übersandte Stellungnahme der BT (Germany) GmbH & Co. oHG vom 09.01.2004, S. 4, abrufbar unter http://www.bundesnetzagentur.de/media/archive/520.pdf (Website vom 30.09.2006), in der darauf verwiesen wird, dass Mietleitungen oft als Synonym für fest definierte Bandbreiten verwendet wird (zur Bandbreite siehe oben S. 21).

[111] So Voss in der Auflage 2004, Das große PC & Internet Lexikon, S. 389.

[112] Siehe zur IP-Adresse oben S. 21.

[113] Lipp, VPN, S. 83; Köhntopp/Köhntopp, CR 2000, 248, 248; siehe auch Blümel/Soldo, Internet-Praxis für Juristen, S. 28 ff.; Göckel in: Königshofen, Das neue Telekommunikationsrecht in der Praxis, S. 127 Fn. 4.

[114] Bei einem Browser handelt es sich um ein Programm, das den Zugriff bzw. den Aufruf von Websites im World Wide Web (WWW) ermöglicht, siehe Voss, Das große PC & Internet Lexikon 2007, S.888.

[115] Zu Domain-Namen bei einem VPN siehe beispielsweise das Angebot von T-Online (vgl. S. 2 Fn. 9) „directVPN Administrator-Benutzerhandbuch“, S. 10 sowie das Angebot von T-Online, abrufbar unter ftp://software.t-online.de/pub/service/business/cs/vpn/securevpn-benutzerhandbuch.pdf, S. 236 ff. (Website vom 30.09.2006), im Folgenden: „SecureVPN-Benutzerhandbuch“.

bezüglich der registrierten Domain-Namen und der zugehörigen IP-Adressen enthalten sind.[116] Sein DNS-Server wird regelmäßig aktualisiert und mit dem DNS-Server der DENIC[117] abgeglichen, um neu vergebene Internet-Adressen im Internet finden zu können.[118]

d. Router

Auch Server, die das Routing übernehmen, gehören zur notwendigen Internet-spezifischen Infrastruktur.[119] Router dienen dazu, die Daten zwischen Sender und Empfänger im Internet zu transportieren.[120] So werden Router-Rechner entweder als „Wegpunkte" für Datenpakete beschrieben, die entscheiden sollen, welche Route ein Datenpaket vom Absender zum Empfänger nimmt.[121] Router werden aber auch als Geräte zur Kopplung verschiedener Netze definiert, die Datenpakete auf der günstigsten Route zu ihrem Ziel leiten.[122]

---

[116] Siehe hierzu auch das Urteil des OLG Hamburg, MMR 2000, 278, 278.

[117] Der Provider vergibt im eigentlichen Sinne nicht Domain-Namen. Dies ist vielmehr in Deutschland die Aufgabe der DENIC, Network Information Center für Deutschland, mit Sitz in Frankfurt, die für die Verwaltung sämtlicher Domain-Namen in Deutschland zuständig ist. Der Provider kann bei der DENIC die gewünschten Domain-Namen beantragen, die er an seine Kunden weitergibt. Für die Verwaltung aller weltweit vergebenen Domain-Namen ist ICANN zuständig (Internet Corporation for Assigned Numbers and Names mit Sitz in Kalifornien; im Oktober 1998 wurde ICANN gegründet). Vgl. zu den Aufgaben der DENIC auch Göckel in: Königshofen, Das neue Telekommunikationsrecht in der Praxis, S. 132; Bücking, Namens- und Kennzeichenrecht im Internet (Domainrecht), S. 20/21. Zu den Aufgaben der IANA (Internet Assigned Numbers Authority) als Vorgängerorganisation der ICANN siehe Göckel in: Königshofen, Das neue Telekommunikationsrecht in der Praxis, S. 129 und Bücking, Namens- und Kennzeichenrecht im Internet (Domainrecht), S. 13/14. Bei Kloepfer, Informationsrecht, § 6 Rn. 84 ff. finden sich Einzelheiten zur Funktion der ICANN.

[118] Siehe zu DNS Voss, Das große PC & Internet Lexikon 2007, S. 244/245, der ausführt, dass der gesamte Datenbestand nicht auf jedem DNS-Server liegt, sondern das System kaskadenartig aus aufeinander aufbauenden DNS-Servern zusammengesetzt ist. Die DNS-Server mit der höchsten Priorität, die die Basis dieses Systems bilden, werden als Rootserver bezeichnet und stehen meist in den USA, wobei es 13 Stück gibt. Änderungen des Datenbestandes werden nur auf dieser untersten Ebene durchgeführt, und die DNS-Server der oberen Ebenen aktualisieren ihre Datenbestände in bestimmten Zeitabständen (ca. alle drei bis vier Tage) mit denen der niedrigeren Ebene. Voss (aaO) verweist ebenso darauf, dass es einige Tage dauern kann, bis ein neuer Domain-Name (oder der Wechsel einer zugrundeliegenden IP-Adresse) weltweit auf den DNS-Servern aller Internetzugangsprovidern aktualisiert wurde.

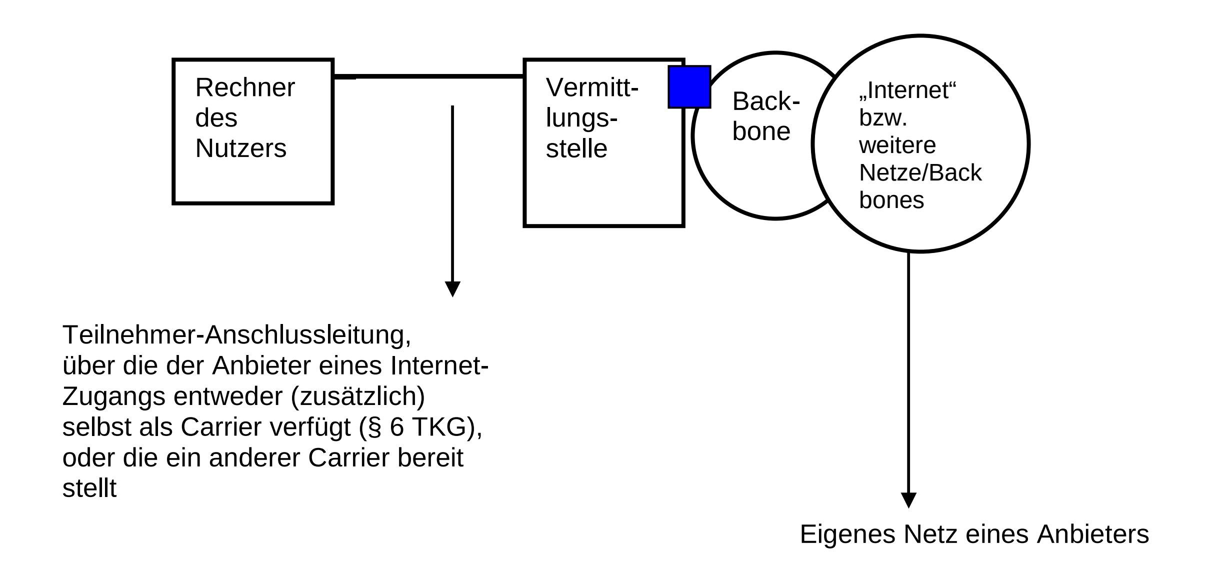
[119] Köhntopp/Köhntopp, CR 2000, 248, 249.

[120] Koch, CR 1997, 193, 199. Zur paketvermittelte Datenübertragung sieheS. 20.. Siehe auch Ehmann/Helfrich, EG-Datenschutzrichtlinie, Artikel 4 Rn. 10, die darauf hinweisen, dass im vorhinein oftmals nicht klar sei, welchen Weg, die einzelnen Pakete nehmen, da Datenübermittlung im Internet regelmäßig danach bestimmt wird, welche Datenwege über möglichst große freie Übertragungskapazitäten verfügen oder zum Zeitpunkt der Übertragung am geringsten ausgelastet sind.

[121] Pankoke, Von der Presse- zur Providerhaftung, S. 56.

[122] Campo/Pohlmann, Virtual Private Networks, S. 384.

e. Beispiel „Vereinfachte Darstellung der Internetverbindung“



■ Übergabepunkt (PoP) zum Backbone eines Anbieters

Insgesamt ist zu berücksichtigen, dass es sowohl Backbone-Betreiber gibt, die nicht zugleich Carrier sind, als auch Anbieter, die zwar Internetzugangsknoten besitzen, aber nicht über ein eigenes Backbone verfügen.[123]
Zur Bereitstellung des Internetzugangs über das Telefonnetz ist somit unerheblich, ob der Anbieter des Internetzugangs über angemietete oder gar eigene Zugangsleitungen zur Vermittlungsstelle und/oder über ein eigenes Backbone verfügt. Wichtig ist lediglich, dass er die entsprechende Infrastruktur in Form von Internetzugangsknoten bereitstellen kann. Diese Bereitstellung kann ebenso durch einen „virtuellen Provider“ erfolgen, der zwar einen Internetzugang zur Verfügung stellt, aber die Infrastruktur eines anderen Anbieters nutzt.[124] Er übernimmt in diesem Falle nur die Verwaltung.

[123] Siehe die Übersicht bei Summa in: Holznagel/Nelles/Sokol, TKÜV, S. 25.
[124] Zum Begriff des „virtuellen“ Internet Service Provider siehe auch Summa in: Holznagel/Nelles/Sokol, TKÜV, S. 25.

II. Technische Details von VPN

Ein Internet-VPN besteht neben der Bereitstellung eines Internetzugangs über Telekommunikationsnetze[125] aus weiteren technischen Details, die im Folgenden näher dargestellt werden. Entsprechend den Ausführungen bei der Internetverbindung ist ebenso hier ein vereinfachter Aufbau gewählt worden, wie er für die anschließende rechtliche Prüfung erforderlich ist.[126]

1. Tunnel und Tunneling-Protokolle

Für den Einsatz eines VPN gibt es generell zwei vorrangige Gründe:
Ein wichtiger Grund ist die Datensicherheit und die mit einem VPN verbundene Möglichkeit, Daten gegen Zugriffe durch Dritte gesichert zu versenden.[127]
Ein anderer Grund liegt darin, dass Unternehmensstandorte oftmals mit anderen Netzwerkprotokollen als TCP/IP[128] arbeiten und damit andere Regelsätze als die des Internet verwenden.[129]
Zu diesem Zweck werden so genannte Datentunnel geschaffen, wobei eine VPN-Verbindung insgesamt auch als Tunnel bezeichnet wird.[130]
Tunnel bedeutet letztendlich, dass einzelne Datenpakete[131] „wie durch einen (IP-)Tunnel“ durch das Internet geschleust werden, da sie beim Versender in ein weiteres Datenpaket, und zwar des Protokolls IP, mit welchem das Internet arbeitet, eingepackt werden, und beim Empfänger wieder ausgepackt werden.

---

[125] Ergänzend sei angemerkt, dass für die Anbindung der Standorte eines VPN an das Internet ebenfalls die Einwahl über das Mobilfunknetz in Betracht kommen. Jedoch erfolgt auch hier die Einwahl per Handy bis zum nächsten Internetzugangsknoten (vgl. zur mobilen Einwahlmöglichkeit über Handy bis zum nächsten PoP das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 23/28).
[126] Vgl. S. 25.
[127] Roth/Haber, ITRB 2004, 19, 20; Schneider, MMR 1999, 571, 575; siehe auch Lipp, VPN, S. 45/46.
[128] Siehe hierzu auch S. 20.
[129] Siehe hierzu Buckbesch/Köhler, Virtuelle Private Netze, S. 21/34, die beispielsweise auf Protokolle wie NetBEUI und IPX verweisen. NetBEUI ist die Abkürzung für NetBIOS Extended User Interface (siehe Voss, Das große PC & Internet Lexikon 2007, S. 552), IPX bedeutet Internet Packet Exchange (vgl. Campo/Pohlmann, Virtual Private Networks, S. 377). Zum Begriff des Protokolls siehe S. 19, wo bereits dargestellt worden ist, dass sich Rechner und Rechnernetzwerke lediglich dann verständigen können, sofern sie gleiche Regelsätze bzw. Protokolle anwenden.
[130] Vgl. Lipp, VPN, S. 166 ff.; Roth/Haber, ITRB 2004, 19, 20; Schneider, MMR 1999, 571, 575.
[131] Im Internet erfolgt eine paketvermittelte Datenübertragung (vgl. S. 20). Siehe zur Paketvermittlung außerdem: Tanenbaum, Computernetzwerke, S. 174 ff.

Durch entsprechendes Verpacken kann ein hohes Maß an Übertragungssicherheit erreicht werden.

Um die Voraussetzung für das Einkapseln der Datenpakete zu schaffen, sind Tunneling-Protokolle notwendig. Tunneling-Protokolle sind in der Transport- und/oder Anwendungsschicht des OSI-Schichtenmodellsangesiedelt.[132]
Jedes Tunneling-Protokoll stellt hierbei ein Verfahren zum Transport von Datenpaketen über andere Netze dar.[133]
Die unterschiedlichen Protokolle nutzen lediglich für die Verwirklichung dieses Datentransports verschiedene Schichten des OSI-Schichtenmodells mit der Konsequenz, dass die einzelnen Tunneling-Protokolle dem Nutzer unterschiedliche Funktionen bieten.

Ergänzend ist hier außerdem auf das MPLS-Verfahren (Multi Protocol Label Switching) hingewiesen, welches Backbone-Betreiber[134] in ihren Backbone-Netzen einsetzen.[135]
MPLS wird regelmäßig im Zusammenhang mit der Verwirklichung eines VPN und einem Datentunnel genannt.[136] Hierbei handelt es sich jedoch nicht im eigentlichen Sinne um ein Tunneling-Protokoll,[137] sondern es wird vorrangig eingesetzt, um schnellere Datenübertragung auf fest definierten Routen innerhalb des Backbones zu erreichen. In großen Netzen mit zunehmend höheren Geschwindigkeiten wird dieses Verfahren zur Verbesserung der Performance eingesetzt.[138]

---

[132] Siehe zu den einzelnen Schichten des OSI-Schichtenmodells, S. 22 ff.
[133] Böhmer, Virtual Private Networks (2. Auflage), S. 206.
[134] Siehe zum Begriff des Backbones S. 28 ff.
[135] Siehe Lipp, VPN, S. 174/175. Vgl. zum Begriff des MPLS außerdem Buckbesch/Köhler, Virtuelle Private Netze, S. 122; Böhmer, Virtual Private Networks (2. Auflage), S. 380 ff. MPLS wird beispielsweise angeboten von COLT TELECOM GmbH abrufbar unter http://www.colt.net/de/ge/produkte/data_/colt_ip_vpn_corporate; Arcor AG & Co.KG abrufbar unterhttp://www.arcor.de/business/enterprise/fnetz/net_det.jsp ; Cable & Wireless Telecommunication Services GmbH abrufbar http://www.cw.com/europe/services/carrier_mpls.html;
Claranet GmbH abrufbar unter http://www.claranet.de./ipservices/vpn/vpn_mpls.php (alle Websites vom 30.09.2006).
[136] Buckbesch/Köhler, Virtuelle Private Netze, S. 122; Lipp, VPN, S. 174/175; Böhmer, Virtual Private Networks (2. Auflage), S. 380 ff.
[137] Lipp, VPN, S. 175.
[138] Lipp, VPN, S. 174; vgl. auch Böhmer, Virtual Private Networks, S. 56 ff., insbesondere S. 70 (in der 1. Auflage) sowie S. 302 in der 2. Auflage.

Dieses Verfahren kann den Schutz der Privatsphäre insoweit herstellen, indem durch die Hinzufügung eines MPLS-Headers eine korrekte Weiterleitung der IP-Datenpakete innerhalb des Backbones über fest definierte Routen erfolgt, die nicht verlassen werden können.[139]

Insgesamt geht es beim Einsatz von MPLS im Rahmen von VPN weniger darum, die zu übertragenden Daten zu verschlüsseln, als den Datenverkehr logisch voneinander zu trennen und individuell zu behandeln.[140]

Eine Verschlüsselung der Daten muss daher durch den Einsatz zusätzlicher Protokolle durchgeführt werden.[141]

a. Datentransport

Das Layer-2-Tunneling Protokoll (L2TP) bezieht sich auf die Schicht 2 des OSI-Schichtenmodells[142] (Data-Link-Layer bzw. Verbindungsschicht) und kann Pakete dieser Schicht verkapseln.[143]

Dieses Protokoll wird regelmäßig als standardisiertes Tunneling-Protokoll bezeichnet und stets im Zusammenhang mit der Konzeption eines VPN genannt,[144] so dass es hier anstelle von anderen, nicht standardisierten[145] Protokollen dargestellt werden soll. Andere nicht standardisierte Tunneling-Protokolle, die auf der Schicht 2 des OSI-Schichtenmodells arbeiten, sind

---

[139] Vgl. Tanenbaum, Computernetzwerke, S. 457 ff.; Lienemann, Virtuelle Private Netzwerke, S. 129.

[140] Lienemann, Virtuelle Private Netzwerke, S. 129.

[141] Siehe zum Vergleich zwischen IPSec und MPLS auch die Informationen unter http://www.claranet.de./ipservices/vpn/. Ein Vergleich zwischen IPSec und MPLS findet sich ebenso bei Böhmer, Virtual Private Networks (2. Auflage), S. 379 ff. Auf S. 380 wird darauf hingewiesen, dass IPSec auch in Verbindung mit MPLS eingesetzt werden kann.

[142] Siehe zum OSI-Schichtenmodell S. 22 ff.

[143] Vgl. Lipp, VPN, S. 172/173.

[144] Siehe etwa Lienemann, Virtuelle Private Netzwerke, S. 117 ff.; Lipp, VPN, S. 171 ff.;; Buckbesch/Köhler, Virtuelle Private Netze, S. 30 ff.

[145] Der Begriff „Standard" ist jedoch mit Vorsicht zu genießen, da es sich hierbei weder um eine ISO-Zertifizierung noch um eine DIN-Norm, also eine anerkannte Standardisierung gemäß der Internationalen Standardisierungsorganisation bzw. des Deutschen Institutes für Normung handelt. Vielmehr regelt hier die Internet-Gemeinschaft selbst, welche Technik sie als am besten geeignet im Rahmen der Internetnutzung einstuft. Hierbei ist jedoch fraglich, ob damit zwangsläufig ein objektiver Maßstab für die Geeignetheit eines Verfahrens oder Protokolls besteht. Denn die (IETF)" verbreitet zwar regelmäßig Vorschläge und Informationen in Form von RFCs (siehe hierzu bereits S. 28 Fn. 100). Problematisch ist hierbei allerdings, dass diese Gruppierung eine für jedermann offene Organisation darstellt, die weder einen formellen Status noch formelle Mitgliedschaftsregeln besitzt (vgl. auch http://www.ietf.org, Website vom 30.09.2006). Bei der Klärung technischer Detailfragen und Problemlösung kann sich also jeder zu Wort melden, wobei es nahe liegt, dass sich hierbei auch konkurrierende Unternehmen gegenüberstehen können, die daran interessiert sind, ihre jeweiligen Produkte zu „verkaufen". Dies sollte bezüglich der Aussagekraft von RFCs stets berücksichtigt werden.

beispielsweise das Point-to-Point-Tunneling-Protocol (PPTP) und das Layer-2 Forwarding Verfahren (L2F).[146]

Eine Verkapselung mittels L2TP wäre dann überflüssig, sofern zwei Rechner per Wählleitung oder per Festverbindung (im Sinne einer Punkt-zu-Punkt-Verbindung)[147] miteinander verbunden wären. Denn dann würde die Übertragung keine zusätzliche Verkapselung benötigt werden, da das auf der Schicht 2 (Verbindungsschicht) ebenfalls arbeitende[148] und oben beschriebene Einwahlprotokoll PPP in Lage ist, auch andere Netzwerkprotokolle als IP zu übertragen.[149]

So gibt es beispielsweise die Möglichkeit, dass ein Unternehmen seinen eigenen Einwahlservice (bzw. sein eigenes Einwahlgerät - Remote Access Concentrator) in das Unternehmensnetz betreibt und die Verbindung der Standorte allein über Telefonleitungen erfolgt.[150]

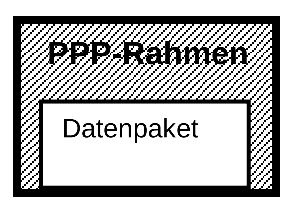
Bei einer solchen Standortverbindung bzw. Punkt-zu-Punkt-Verbindung mittels Telefonleitung ermöglicht PPP demgemäß auf der zweiten Schicht des OSI-Schichtenmodells die Versendung von Daten, die mittels auf Schicht 3 des OSI-Schichtenmodells arbeitenden Netzwerkprotokollen erstellt worden sind. Auf Schicht 3 des OSI-Schichtenmodells arbeitende Netzwerkprotokolle, die in vielen Unternehmen eine Rolle spielen, sind beispielsweise IP, NetBEUI, SNA, IPX oder Appletalk, [151] - je nachdem für welchen Regelsatz bzw. Sprache sich das jeweilige Unternehmen als Betreiber eines Netzwerksystems entschieden hat.

Bei diesem Prozess wird ein so genannter PPP-Rahmen für den Datentransport über die Punkt-zu-Punkt-Verbindung geschaffen,[152] der dafür verantwortlich ist, dass die Daten transportiert werden können.

---

[146] Siehe hierzu Böhmer, Virtual Private Networks (2. Auflage), S. 210 ff.; Campo/Pohlmann, Virtual Private Networks, S. 159 ff.; Lipp, VPN, S. 176, 178; Buckbesch/Köhler, Virtuelle Private Netze, S. 119/121. Als nicht standardisiertes Tunneling-Protokoll wird außerdem das Protokoll Bay-DVS genannt (Lipp, VPN, S. 176/404).
[147] Siehe zum Begriff „Punkt-zu-Punkt“ S. 21.
[148] Lipp, VPN, S. 283.
[149] Lipp, VPN, S. 277.
[150] Dies stellt eine Punkt-zu-Punkt-Verbindung dar (siehe hierzu auch S. 21 sowie Lipp, VPN, S. 37/38.
[151] Vgl. Lipp, VPN S. 178/277; Buckbesch/Köhler, Virtuelle Private Netze, S. 21.
[152] Siehe Lipp, VPN, S. 172.

PPP schafft dementsprechend die technischen Voraussetzungen dafür, dass die mittels unterschiedlicher Netzwerkprotokolle erstellten Daten bei einer Punkt-zu-Punkt-Verbindung übertragen werden.



Sofern aber ein Unternehmen Kosten sparen und daher auf eine Standardfestverbindung oder Wählverbindung über das öffentliche Telefonnetz zwischen den Unternehmensstandorten mittels Telefonleitungen verzichten möchte, die regelmäßig mit hohen Verbindungsgebühren verbunden sind,[153] kommt als Alternative eine Telefonverbindung zum nächst gelegenen PoP bzw. Einwahlserver mit darauf folgender Verbindung über das Internet in Betracht.[154] Insbesondere kann eine Einwahl am PoP meist zu einem Ortstarif erfolgen.[155]

Beispiel:

Das Unternehmen A hat sich für das Netzwerkprotokoll NetBEUI in seiner Hauptzentrale in Hamburg entschieden, wobei seine Filiale A1 in München gleichfalls mit NetBEUI arbeitet. Wenn A nun wegen der Kostenersparnis die Verbindung über das Internet wählt, jedoch das Protokoll des Unternehmens A „NetBEUI" und das Internet-Protokoll „IP" nicht übereinstimmen, wäre an sich wegen unterschiedlicher „Sprache"[156] kein Datenaustausch möglich.

---

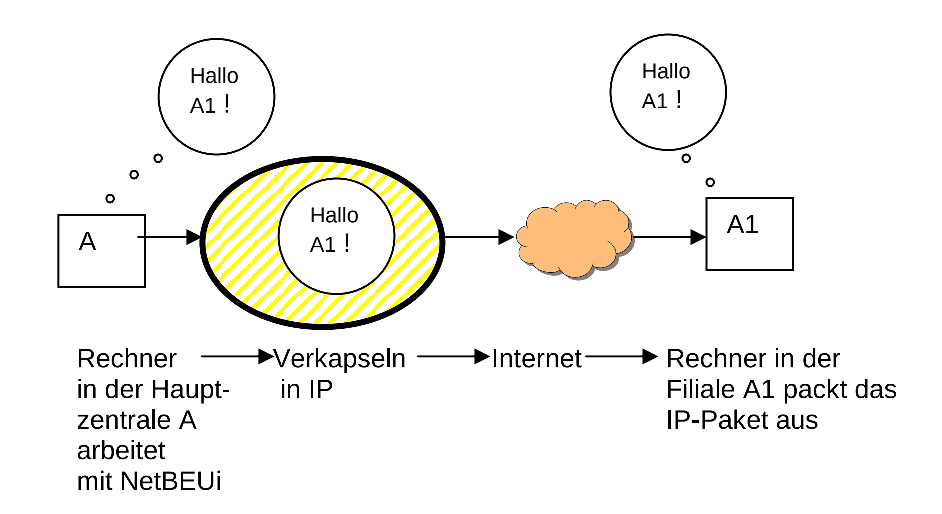
[153] Eine Datenverbindung und Datenaustausch unmittelbar zwischen A sowie A1 durch eine Telefonverbindung ist zwar mittels des PPP-Protokolls grundsätzlich möglich, jedoch regelmäßig mit hohen Kosten verbunden. Siehe auch Lipp, VPN, S. 37/38, der auf die hohen Grundgebühren und Verbindungsgebühren, besonders im Fernbereich, bei dieser Alternative hinweist, insbesondere auf die Kostenintensität beim Betrieb der hierfür notwendigen eigenen Einwahlsysteme an den jeweiligen Standorten durch denjenigen, der das VPN für sein Unternehmen einrichten möchte. Eine unmittelbare Verbindung von Standorten mittels Festverbindungen bzw. Standleitungen hat den Vorteil ständiger Übertragungsbereitschaft, jedoch ebenso den Nachteil der hohen Kosten, da in der Regel anhand der Länge der Strecke abgerechnet wird, die für die direkte Anbindung benötigt wird (vgl. zur Standleitung als fest geschalteter physikalischer Übertragungsweg auch Piepenbrock in: TKG-Kommentar (2. Auflage), Glossar S. 1579). Siehe zur Standleitung auch S. 29.
[154] Vgl. Lipp, VPN, S. 40.
[155] Vgl. Lipp, VPN, S. 38.
[156] Siehe S. 19.

Dieses Problem wird durch den VPN-Tunnel mittels L2TP gelöst.[157]

Dieser ermöglicht, dass die Datenpakete der Hauptzentrale A und der Filiale A1 in einem Datenpaket des Internet-Protokolls IP eingeschlossen und transportiert werden.

Das komplette NETBEUI-Datenpaket wird in ein IP-Datenpaket „verpackt“ und kann daher über das Internet versendet werden, da nun die Protokolle übereinstimmen.[158]

Bei dem Empfänger der Daten wird dieses Paket wieder ausgepackt.



A und A1 arbeiten mit dem Netzwerkprotokoll. Die in der Hauptzentrale A mittels des Netzwerkprotokolls NetBEUI generierten Daten („Hallo A1!“) werden komplett in ein IP-Datenpaket eingekapselt und bei A1 wieder ausgepackt,[159] so dass A1 den Text lesen kann.

Verkapselung bedeutet jedoch nicht zwangsläufig Zugriffssicherheit bzw. Datenverschlüsselung.[160]

Die NetBEUI-Datenpakete im obigen Beispielsfalle, die über einen IP-Tunnel versandt werden, sind nicht zwangsläufig verschlüsselt. Soll Datensicherheit erreicht werden, ist der Einsatz von Tunneling-Protokollen notwendig, die zusätzlich zur Datenübertragung eine Verschlüsselung ermöglichen, was im Folgenden dargestellt wird.[161]

---

[157] Vgl. Buckbesch/Köhler, Virtuelle Private Netze, S. 18 mit dem Hinweis, dass VPN-Technologie ermöglicht, mit IP-fremden Netzwerkprotokollen wie etwa IPX, DECnet, Appletalk zu kommunizieren.
[158] Lipp, VPN, S. 166 ff.
[159] Vgl. auch die Ausführungen bei Lipp, VPN, S. 172/178. Siehe Buckbesch/Köhler, Virtuelle Private Netze, S. 23 zu der Möglichkeit die Datenpakete eines Netzwerkprotokolls anstelle von PPP-Rahmen direkt in IP einzupacken.
[160] Lipp, VPN, S. 178.
[161] Lipp, VPN, S. 303/304.

b. Datentransport und Datenverschlüsselung (Datensicherheit)

Auch das IP-Security-Protokoll (IPSec) sowie L2Sec[162] sind als standardisierte[163] (Sicherheits-) Tunneling-Protokolle anerkannt. Ergänzend ist anzumerken, dass es sich bei IPSec nicht nur um einen einzigen Standard handelt, sondern die einzelnen Bestandteile von IPSec sind auf ein ganzes Bündel unterschiedlich kombinierbarer Standards bzw. RFCs (Request for Comments) verteilt.[164]

Es gibt im Rahmen eines VPN noch ein weiteres Sicherheitsprotokoll, welches ebenfalls die Datenverschlüsselung ermöglicht, das Point-to-Point-Tunneling-Protokoll (PPTP). Dieses Protokoll ist jedoch seitens der IETF[165] nicht als standardisiertes Protokoll anerkannt und weist auch nicht die Stärke von IPSec auf, insbesondere war die Ableitung des Schlüssels, mit dem die Daten verschlüsselt werden, aus der Benutzerauthentifizierung in der Vergangenheit Zielscheibe von erfolgreichen Angriffen.[166] IPSec und L2Sec werden momentan als die besten Sicherheitsstandards eingestuft.[167] Zu beachten ist aber, dass es eine absolute Sicherheit im Sinne einer mathematischen Unmöglichkeit der

[162] Siehe das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 208/209, wo L2Sec zum einen als standardisiertes Protokoll und zum anderen als Alternative zu IPSec eingestuft wird sowie zu IPSec aaO S. 211 ff. IPSec arbeitet zusätzlich auf der Netzwerkebene (Schicht 3 des OSI-Schichtenmodells), siehe Buckbesch/Köhler, Virtuelle Private Netze, S. 55 ff. Siehe zu L2Sec auch Böhmer, Virtual Private Networks (2. Auflage), S. 226.

[163] Zum Begriff des „Standards" siehe S. 35 Fn. 145. Zu IPSec siehe Lipp, VPN, S. 178. Siehe auch Böhmer (in der 1. Auflage) Virtual Private Networks, S. 229, der darstellt, dass im Laufe der Zeit mehrere ähnliche Tunneling-Protokolle entwickelt worden sind, von denen sich in der Praxis jedoch hauptsächlich IPSec und L2TP (neben PPTP als nicht standardisiertem Protokoll) durchgesetzt haben. Campo/Pohlmann, Virtual Private Networks, S. 151 verweisen darauf, dass mit dem Protokoll IPSec ein in die Zukunft weisender Standard geschaffen worden ist.

[164] Siehe hierzu Buckbesch/Köhler, Virtuelle Private Netze, S. 55. Siehe zum Begriff RFC S. 28 Fn. 100.

[165] Zum Begriff der IETF siehe S. 28 Fn. 100.

[166] Lipp, VPN, S. 180. Der geringe Verschlüsselungsschutz bei PPTP wird als „fahrlässig" bezeichnet (Böhmer, Virtual Private Networks (2. Auflage), S. 212, der den Begriff „fahrlässig" jedoch nicht im formal juristischen Sinne verwendet), da ein breites Spektrum von Angriffen denkbar ist (vgl. Campo/Pohlmann, Virtual Private Networks, S. 161).

[167] Siehe Böhmer, Virtual Private Networks (2. Auflage), S. 229 mit dem Hinweis, dass zwar darauf verwiesen wird, dass es derzeit keine Alternative zu IPSec gebe (und es besser sei als PPTP und L2TP), aber dass dieses Protokoll dennoch nicht ganz kritiklos gesehen werde. Siehe ebenso die Ausführungen in der Computerwoche vom 21.01.2006 (http://whitepaper.computerwoche.de/index.cfm?pid=1&fk=61&pk=466) mit dem Hinweis, dass sich seit geraumer Zeit Zeitschriftenbeiträge über IPSec häufen. In diesen Artikeln sei immer wieder die Rede davon, dass IPSec der höchste Sicherheits-Standard und das für jede Netzwerk-Topologie uneingeschränkt einsetzbare VPN-Protokoll sei. Die Autoren möchten in ihrem Beitrag jedoch zeigen, dass IPSec nur in ganz bestimmten Umgebungen ohne zusätzliche Erweiterungen eingesetzt werden kann.

Entschlüsselung naturgemäß niemals geben kann.[168] Da IPSec und L2Sec im Gegensatz zu PPTP nicht nur als standardisierte bzw. anerkannte Tunneling-Protokolle bezeichnet sowie als besserer Sicherheitsstandard eingestuft werden,[169] sondern auch in den aktuellen Produktbeschreibungen kommerzieller Anbieter als Tunneling-Protokoll im VPN angeboten werden,[170] wird PPTP hier bei der Darstellung außer Acht gelassen.

IPSec und L2Sec ermöglichen im Gegensatz zu L2TP zusätzlich die Sicherheit bzw. Verschlüsselung der Daten. Bei einem Tunneling-Protokoll wie L2TP wäre es weiterhin notwendig, dass der Kunde zusätzlich seine Daten verschlüsselt.[171]

IPSec ist jedoch lediglich in der Lage ist, das Netzwerkprotokoll IP weiterzuleiten bzw. einzukapseln und kann gerade nicht bewerkstelligen kann, dass Netzwerke, die nicht auf IP basieren, dennoch über das Internet miteinander kommunizieren können. Demnach können nur Unternehmensnetzwerke, die mit dem Netzwerkprotokoll IP arbeiten, IPSec einsetzen. [172] Diese „Schwächen" sollen durch den Einsatz von L2Sec ausgeglichen werden. L2Sec ermöglicht neben IP-Paketen ebenso Daten anderer Netzwerkprotokolle, etwa NetBIOS-, IPX- oder SNA-Daten zu übertragen. also Daten von Netzwerken, die andere Protokolle als IP nutzen.[173] L2Sec sowie IPSec beinhalten beide die Möglichkeit der Datenverschlüsselung und ein Schlüsselmanagement,[174] wobei Schlüsselmanagement bedeutet, dass ein Verfahren sämtliche benötigten Schlüssel zur Verschlüsselung erzeugen, auf Integrität und Authentizität prüfen und dafür Sorge tragen kann, dass diese

---

[168] Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 18.

[169] Vgl. Lipp, VPN, S. 176/178; Buckbesch/Köhler, Virtuelle Private Netze, S. 119/121.

[170] Siehe etwa das Angebot von T-Online „SecureVPN-Benutzerhandbuch" und das Angebot von T-Online, abrufbar unter ftp://software.t-online.de/pub/service/pdf/directVPN_Benutzerhandbuch.pdf sowie die Angebote von Cable & Wireless Telecommunication Services GmbH abrufbar unter http://www.cw.com/docs/services/product_pdfs/internet_vpn.pdf, Claranet GmbH abrufbar unter http://www.claranet.de./ipservices/vpn/vpn_ipsec.php und COLT TELECOM GmbH abrufbar unter http://www.colt.net/de/ge/produkte/data_/colt_ip_vpn_corporate (sämtliche Websites vom30.09.2006).

[171] Siehe zu L2TP S. 35 ff. sowie Lipp, VPN, S. 178/303/304.

[172] Vgl. Buckbesch/Köhler, Virtuelle Private Netze, S. 75.

[173] Siehe das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 208.

[174] Vgl. Lipp, VPN, S. 184 und das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 208/209.

Schlüssel in einem VPN zur richtigen Gegenstelle, also dem richtigen Netzwerk, übertragen werden.[175]
Verschlüsselungsverfahren sind entweder asymmetrisch oder symmetrisch. Asymmetrisch bedeutet, dass zwei jeweils unterschiedliche Schlüssel existieren, und zwar ein privater und ein öffentlicher Schlüssel.[176]
Der private Schlüssel ist geheim und nur demjenigen bekannt, der eine Nachricht zu verschlüsseln hat. Der öffentliche Schlüssel hingegen ist allgemein bekannt und nimmt die Entschlüsselung der Nachricht vor.[177] Hierfür wird der Begriff „Public-Key-Kryptographie“ benutzt.[178] Das bekannteste Public-Key-Verfahren ist das so genannte RSA-Verfahren.[179] Symmetrische Verschlüsselungsverfahren verwenden für die Verschlüsselung von Daten den gleichen Schlüssel.[180] Dies bedeutet, dass den Kommunikationspartnern dieser Schlüssel jeweils vorliegen muss.[181]

VPN mittels IPSec nutzen die hybride Verschlüsselungstechnik, d.h. dass symmetrische und asymmetrische Verschlüsselungsverfahren kombiniert werden.[182] So wird der mittels des symmetrischen Verschlüsselungsverfahren generierte Schlüssel selbst durch einen Algorithmus bzw. durch ein asymmetrischen Verfahren verschlüsselt und über das Internet zum Kommunikationspartner übertragen wird.[183]

---

[175] Vgl. Lipp, VPN, S. 54; Lienemann, Virtuelle Private Netzwerke, S. 81. Siehe zu den Begriffen „Authentizität“ und „Integrität“ auch Jacob, DuD 2000, 5, 10.
[176] Siehe hierzu auch die Definition im Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 253.
[177] Siehe hierzu auch Schaar, Datenschutz im Internet, Rn. 163.
[178] Die Grundpfeiler der Public-Key-Kryptographie sind ungelöste oder schwierige mathematische Probleme. Besonders geeignet sind mathematische Funktionen, die sich in eine Richtung sehr einfach und schnell berechnen lassen, deren Umkehrung hingegen sehr schwierig und langwierig ist (Lipp, VPN, S. 131).
[179] Das RSA-Verfahren ist benannt nach seinen drei Entdeckern, Ronald Rivest, Adi Shamir und Leonard Adleman (Campo/Pohlmann, Virtual Private Networks, S. 69). So sind bei dem RSA-Verfahren gewisse Teile der Schlüssel bekannt, so dass aufgrund dieser bekannten Elemente der jeweils geheime Teil des anderen Schlüssels berechnet wird (Lipp, VPN, S. 136 ff.).
[180] Campo/Pohlmann, Virtual Private Networks, S. 67; Lipp, VPN, S. 191; siehe auch die Definition im Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 265. Symmetrische Verschlüsselungsverfahren ist beispielsweise der DES-Algorithmus (Data Encryption Standard) bzw. Triple-DES-Algorithmus (Campo/Pohlmann, Virtual Private Networks, S. 68).
[181] Mit dem so genannten Diffie-Hellman-Verfahren ist es möglich, den Schlüssel (d.h. den symmetrischen Schlüssel) auf beiden Seiten zu erzeugen (Lipp, VPN, S. 225). Dieses Verfahren ist ebenfalls nach seinen Entdeckern benannt: Whitfield Diffie und Martin Hellman (vgl. Lipp, VPN, S. 130).
[182] Campo/Pohlmann, Virtual Private Networks, S. 71/82/150.
[183] Campo/Pohlmann, Virtual Private Networks, S. 150; Lipp, VPN S. 131.

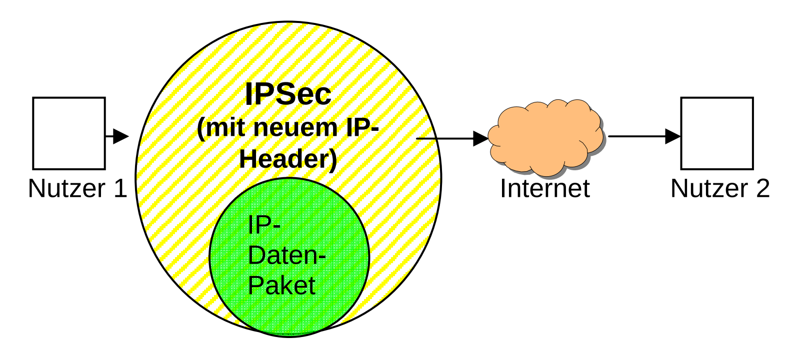
Dieser Schlüsselaustausch findet bei IPSec regelmäßig aufgrund des Schlüsselaustauschprotokolls IKE (Internet Key Exchange) oberhalb der Sitzungsschicht[184] (Schicht 5 des OSi-Schichtenmodells) statt.[185] IKE ist ein Bestandteil des aus mehreren Standards bestehenden IPSec-Protokolls.[186]
Ein Schlüssel ist im Übrigen nichts anderes als eine Regel, nach der die Verschlüsselung der Nachricht erfolgt. Es wird mittels eines Algorithmus eine geheime Zahl erzeugt, die in unterschiedlicher Länge auftreten kann und quasi eine Zusatzinformation zu dem Nachrichtentext darstellt.

Das Entscheidende bei IPSec sowie L2Sec ist außerdem, dass die Möglichkeit besteht, die IP-Pakete des privaten Netzwerkes durch Einfügung eines neuen IP-Headers vollständig in andere IP-Pakete einzukapseln. Header ist der Kopf des Datenpakets, der die Absende- und die Zieladresse enthält.[187]
Die Folge ist, dass die Informationen des Originalpaketes für Dritte nicht sichtbar sind, also weder die übersandten Daten noch die privaten bzw. originalen Netzwerkadressen des Absenders, da diese vollständig verschlüsselt sind.[188] Die einzig sichtbare Information bezieht sich lediglich auf die Gesamtmenge an Paketen, die versendet worden sind.[189]

---

[184] Vgl. zum OSI-Schichtenmodell S. 22 ff.
[185] Siehe hierzu das Schaubild bei Böhmer (in der 1. Auflage) Virtual Private Networks, S. 216 sowie die weiteren Ausführungen auf S.250. Lipp, VPN, S. 94/200 bezeichnet IKE ebenso als Sicherheitsprotokoll. Campo/Pohlmann, Virtual Private Networks, S. 166 verweisen darauf, dass IPSec mit einer Reihe von Algorithmen zum Schlüsselaustausch zusammenarbeitet, wobei das am weitesten verbreitete Verfahren IKE ist. Vgl. zu IKE und IPSEC außerdem Buckbesch/Köhler, Virtuelle Private Netze, S. 68; Böhmer, Virtual Private Networks (2. Auflage), S. 248. Siehe hierzu außerdem das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 222, wo mittels Bilddarstellung dieses Verfahren erklärt wird. Vgl. ebenso die Definition im Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 258, wo darauf verwiesen wird, dass IKE als Bestandteil von IPSec für ein sicheres Schlüsselmanagement verantwortlich ist.
[186] Vgl. S. 39 und die dort zitierten Ausführungen von Buckbesch/Köhler, Virtuelle Private Netze, S. 55 unter Bezug darauf, dass IPSec aus mehreren Standards besteht.
[187] Siehe zu diesem Begriff Schneider, MMR 1999, 571, 571; Pankoke, Von der Presse- zur Providerhaftung, S. 41, der den Header als Briefumschlag mit Absender- und Empfängeradresse bezeichnet.
[188] Siehe Lipp, VPN, S. 203, der darstellt, dass Dritte dadurch keine Informationen über die originalen Adressen erhalten, so dass Angriffe auf das Unternehmensnetzwerk erschwert werden (siehe hierzu auch Lipp, VPN, S. 53/54 mit dem Hinweis, dass Datenvertraulichkeit ebenso erfordert, dass das interne Netzwerk mit seinen Verkehrsbeziehungen, etwa Quell- und Zieladressen, nicht ausgespäht werden kann; vgl. außerdem Campo/Pohlmann, Virtual Private Networks, S. 153 mit dem Hinweis, dass die echten IP-Adressen einem Angreifer verborgen bleiben).
[189] Siehe Böhmer (in der 1. Auflage) Virtual Private Networks, S. 262 mit dem Hinweis, dass IPSec lediglich im Gateway implementiert sein muss und nicht in den lokalen Netzen, so dass ein Angreifer nur die Möglichkeit hat, die Anfangs- und Endpunkte des IPSec-Tunnels festzustellen. Vgl. auch Lipp, VPN, S. 190 mit dem Hinweis, dass ein „Angreifer" als einzige

Diese Möglichkeit besteht allerdings nur im so genannten Tunnelmodus von IPSec. Beim weiteren Betriebsmodus von IPSec, dem Transportmodus, erfolgt ausschließlich eine Verschlüsselung des Datenteils, ohne den Header auszuwechseln.[190]



Nutzer 1 verkapselt mit Hilfe des Tunneling-Protokolls IPSec seine Daten und versendet sie über das Internet zu Nutzer 2.
Das Tunneling-Protokoll IPSec ermöglicht, IP-Datenpakete in ein neues IP-Datenpaket zu verkapseln. Dadurch erhält das Datenpaket einen anderen Absender, und die ursprüngliche IP-Adresse des Absenders wird verborgen. Zusätzlich werden die Daten des Datenpakets verschlüsselt.

2. VPN-Kommunikation

Für ein VPN gilt, wie bei der herkömmlichen Einwahl in das Internet, das Client-Server-Prinzip. Eine Stelle muss die VPN-Verbindung initiieren, also aktiv aufbauen (Client). Eine andere Stelle muss die VPN-Verbindung entgegennehmen bzw. terminieren (Server).
Diesbezüglich kommen bei einem VPN unterschiedliche technische Möglichkeiten in Betracht, wobei im Rahmen dieser Arbeit nur die VPN interessieren, die auf dem Internet basieren.[191]

Information die Gesamtmenge an Paketen, die zwischen Gateway und Host versendet werden, ermitteln kann.

[190] Lienemann, Virtuelle Private Netzwerke, S. 85. Zu den zwei unterschiedlichen IPSec-Betriebsmodi (Tunnel- und Transportmodus) siehe ebenso Lipp, VPN, S. 203 ff. und der Ausführung, dass nur im Tunnelmodus von IPSec ein neuer IP-Header erzeugt wird und der Transport-Modus meistens nur in Intranet- (also nicht Internet-) VPNs genutzt wird (aaO S. 204/205). Siehe außerdem das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 208/209.

[191] Vgl. hierzu die Ausführungen in der Einführung, S. 2. Zu den anderen VPN-Varianten und Kommunikationsstrukturen, wie etwa die Realisierung eines VPN ausschließlich auf der Basis der Technologien von ISDN, Frame Relay oder ATM (Asynchronous Transfer Mode), siehe Lipp, VPN, S. 20 ff., der die Unabhängigkeit von physikalischen Infrastrukturen sowie die niedrigen Betriebskosten als Vorteil der Internet-VPN hervorhebt (aaO S. 24). Internet-VPN werden gerade aus dem Grunde eingesetzt, um die mit höheren Kosten verbundenen Technologien (ISDN, Frame Relay, ATM) zu ersetzen. Sofern das System allein (ohne Nutzung

Die nachfolgenden VPN-Varianten sind dabei in unterschiedliche und denkbare Outsourcing- Möglichkeiten unterteilt.

a. Gateway-VPN

aa. Beispiel

In der folgenden Zeichnung ist gut zu erkennen, wie ein Internet-VPN aufgebaut sein kann. Es ist hier ein Aufbau ausgewählt worden, der der überwiegenden Darstellung eines Gateway-VPN entspricht.[192] Hierbei erfolgt die Verbindung zum Internet mittels des Telefonnetzes,[193] da für den Zugang ins Internet als häufigste Methode die Wählleitung oder DSL-Leitung über das Telefonetz in Betracht kommt.[194] Dies gilt insbesondere für kleinere und mittelständische Unternehmen, die auf kostenintensive Festverbindungen bzw. Standleitungen ins Internet verzichten möchten.[195]

---

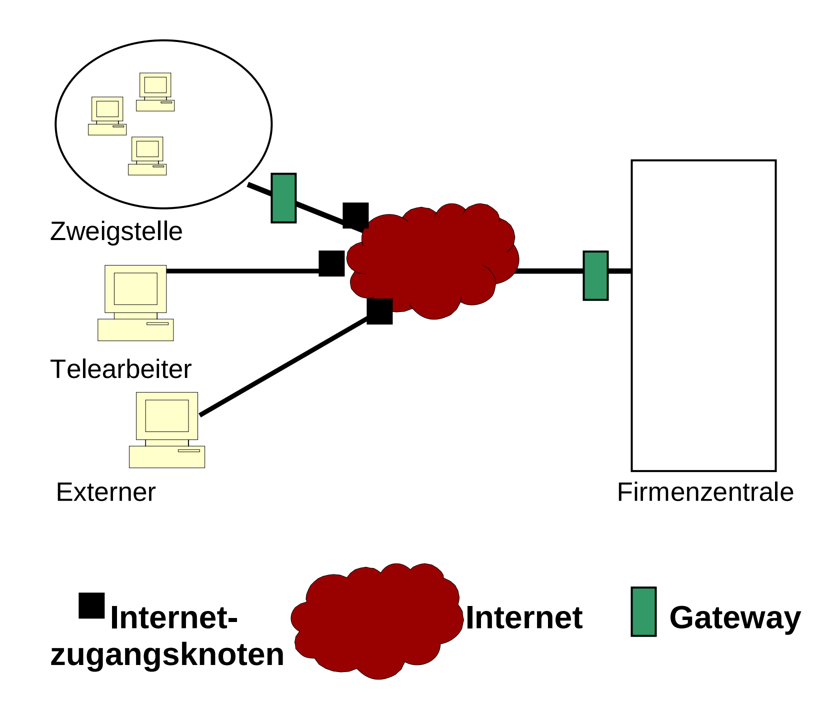
des Internets) an öffentliche Telefonnetze angeschlossen ist (ISDN) und eine eigene Kommunikationsinfrastruktur durch eigene Systeme aufgebaut wird, ist dies regelmäßig mit hohen Verbindungsgebühren und teurer Technologie verbunden (vgl. Lipp, VPN, S. 37/38, der auf die Kostenintensität beim Betrieb eigener Einwahlsysteme (Remote Access Concentrator) eingeht; ebenso Davis, IPSec, S. 290, der auf die enormen Kosten von Telefonleitungen hinweist). Campo/Pohlmann, Virtual Private Networks, S. 41 ff., stellen vergleichend die Vor- und Nachteile von eigener Kommunikationsinfrastruktur (Frame Relay-Netze und ATM-Netze) und öffentlicher Kommunikationsinfrastruktur (Internet) dar und bewerten auch die hohen Investitionskosten, Betriebs- und Wartungskosten als nachteilig (vgl. zu den hohen Kosten von ATM auch die an die Regulierungsbehörde für Post und Telekommunikation (Bundesnetzagentur) übersandte Stellungnahme der BT (Germany) GmbH & Co. oHG vom 09.01.2004, S. 8, abrufbar unter http://www.bundesnetzagentur.de/media/archive/520.pdf (Website vom30.09.2006). Siehe jedoch auch das Angebot von arcor zur Anbindung von Standorten über ATM unter http://www.arcor.de/pdf/arcor/business/enterprise/fnetz/dblatt_atm_fr_lancon.pdf (Website vom 30.09.2006)

[192] Siehe hierzu etwa Lipp, VPN, S. 44/171; Buckbesch/Köhler, Virtuelle Private Netze, S. 13-15; Davis, IPSec, S. 291; Campo/Pohlmann, Virtual Private Networks, S. 136 ff.;; Lienemann, Virtuelle Private Netzwerke, S. 35 ff.).

[193] Auch für ein VPN besteht darüber hinaus die Kombinationsmöglichkeit mit einem W-LAN, da entsprechende Abschirmmechanismen durch Verschlüsselungsprotokolle (vom Rechner ausgehend bis hin zur Telefonanschlussdose und darüber hinaus) bereits entwickelt sind (vgl. Röhrborn/Katko, CR 2002, 882, 887 Fn. 43).

[194] Siehe hierzu S. 25.

[195] Siehe zur Standleitung/Mietleitung S. 29. Siehe außerdem die an die Regulierungsbehörde für Post und Telekommunikation (Bundesnetzagentur übersandte Stellungnahme der BT (Germany) GmbH & Co. oHG vom 09.01.2004, S. 4/8, abrufbar unter http://www.bundesnetzagentur.de/media/archive/520.pdf (Website vom30.09.2006), in der darauf verwiesen wird, dass Mietleitungen circa 30-55% teurer sind als DSL) oder auf die oben genannten und ebenso kostenintensiven ATM- sowie Frame Relay Technologien (siehe Fn. 191 sowie die an die Regulierungsbehörde für Post und Telekommunikation (Bundesnetzagentur) übersandte Stellungnahme der BT (Germany) GmbH & Co. oHG vom 09.01.2004, S. 8, abrufbar unter http://www.bundesnetzagentur.de/media/archive/520.pdf (Website vom30.09.2006). Vgl. außerdem Buckbesch/Köhler, Virtuelle Private Netze, S. 112 mit dem



In diesem Beispiel haben Zweigstelle, Telearbeiter und Externe (wie beispielsweise Lieferanten oder freie Mitarbeiter, die nicht in das Unternehmen eingegliedert sind) die Möglichkeit über Einwahl in einen Internetzugangsknoten, PoP, eines Anbieters von Internet-Zugängen (z.B. T-Online oder AOL) und anschließender Weitervermittlung ins Internet, Zugriff auf den Server einer Firmenzentrale zu nehmen. Hierbei werden Datentunnel aufgebaut, die, beispielsweise mittels IPSec, verschlüsselt werden können.[196]
Der Zugriff auf den Internetzugangsknoten erfolgt über Wählverbindung und das Telefonnetz, was in dem Bildbeispiel durch Verbindungslinien zwischen der Zweigstelle, dem Telearbeiter (die im häuslichen Bereich tätig sein können), dem Externen sowie dem Internetzugangsknoten dargestellt ist.[197]

Hinweis, dass durch (Internet-) VPN teure Standleitungen und Wählverbindungen abgelöst werden können). Auch eine Wählverbindung (unmittelbar zwischen den Standorten ohne die Nutzung des Internets) über das öffentliche Telefonnetz, verbunden mit dem Einsatz von zusätzlicher, teurer Technologie wie eigenen Einwahlsystemen (Remote Access Concentrator), ist bei Fernverbindungen oder internationalen Verbindungen teurer als die Verbindung zum nächsten PoP zum Ortstarif (vgl. hierzu das Beispiel zu L2TP auf S. 35).

[196] Zu IPSec siehe oben S. 39.

[197] Da ein Internet-VPN den Vorteil hat, von der Netzwerktechnologie der Ebene 2 unabhängig zu sein (Buckbesch/Köhler, Virtuelle Private Netze, S. 12; siehe außerdem die Ausführungen unter Fn. 191), bedeutet dies für das vorliegende Bildbeispiel, dass die Kommunikation neben der hier gewählten Wählverbindung in den nächsten PoP ebenso über ATM oder Frame Relay aufgebaut werden könnte (vgl. auch Lipp, VPN, S. 24; Böhmer, Virtual Private Networks (2. Auflage), S. 9 ff.). Ein Internet-VPN erlaubt, unterschiedliche Technologien an den einzelnen Standorten zu verwenden. Hier zeigt sich ebenso der Vorteil eines Internet-VPN gegenüber einem (ausschließlich) mittels Frame Relay oder ATM-Technologien verwirklichten VPN, da derjenige, der ein VPN aufbauen möchte, bei letzteren technisch auf das jeweilige Übermittlungsverfahren (also Frame Relay oder ATM) an jedem Standort festgelegt ist (Böhmer aaO). Zur Klarstellung sei darauf hingewiesen, dass Technologien wie ATM oder Frame Relay zum einen VPN-Verbindungen ohne Inanspruchnahme des Internet ermöglichen können (Böhmer, Virtual Private Networks, S. 11). Zum anderen ermöglicht ein Internet-VPN jedoch, diese Techniken so mit einzubinden, dass mittels der Netze, die mit diesen Techniken betrieben

Der (verschlüsselte) Verbindungsaufbau erfolgt vom Rechner des Nutzers (Telearbeiter (die im häuslichen Bereich tätig sind), Externer, Nutzer in der Zweigestelle) über das Internet bis hin zu einem Gateway.[198]

Ein Gateway ist die Übergangsstelle zwischen zwei grundsätzlich verschiedenen Netzwerken, im obigen Beispiel zwischen Internet und Zweigstelle sowie Internet und Firmenzentrale.[199]

Bei einem Gateway handelt es sich im Allgemeinen um einen Rechner, der gewissermaßen als Übersetzer zwischen den beiden Netzwerken wirkt.[200] Im Sinne des obigen Beispiels soll in dieser Arbeit hinsichtlich des Endpunktes der Verbindung stets von Gateway die Rede sein.[201] Jedoch haben die Anfangs- und Endpunkte der Verbindungen regelmäßig unterschiedliche Bezeichnungen, abhängig von Protokoll, Standard oder Hersteller.[202] So wird teilweise ebenso der Begriff VPN-Box bzw. Black Box verwandt,[203] oder es werden Router eingesetzt.[204]

---

werden, ein Zugang in das Internet bereit gestellt wird (Buckbesch/Köhler, Virtuelle Private Netze, S. 11/12; Lipp, VPN, S. 24;).

[198] Siehe Lipp, VPN, S. 179/ 182/326 zur Möglichkeit zwischen zwei Gateway (in dem obigen Bildbeispiel: Gateway der Zweigstelle und Gateway der Firmenzentrale) einen Datentunnel aufzubauen.

[199] Siehe auch Hammer, DuD 2003, 240, 240.

[200] Tanenbaum, Computernetzwerke, S. 41 verweist darauf, dass Gateways die für Hardware und Software erforderliche Übersetzung übernehmen und die Verbindung zwischen meist miteinander nicht kompatiblen Netzen vornehmen.

[201] Siehe etwa auch Lipp, VPN, S. 41 ff.; Campo/Pohlmann, Virtual Private Networks, S. 121 ff.

[202] Vgl. Buckbesch/Köhler, Virtuelle Private Netze, S. 22). Siehe zur Definition „Gateway“ außerdem Bizer, DuD 2000, 44, 44, der darstellt, dass es sich bei einem Gateway um einen Vermittlungscomputer handelt, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Vgl. auch Davis, IPSec, S. 290, der bei der Darstellung von VPN den Begriff „Security Gateway“ verwendet und damit einen Zugangspunkt zu einem Netzwerk meint, der nur autorisierten Zugriff erlaubt und sich um die Zugangskontrolle kümmert.

[203] Abel, Praxishandbuch, IT-Know-how für den Datenschutzbeauftragten, Teil 5/2.3.3 S. 2/3. Campo/Pohlmann, Virtual Private Networks, S. 122 .

[204] Anstatt eines Gateway kann auch ein Router eingesetzt werden. Ein Router ist ebenfalls ein Rechner, der in der Lage ist, zwei oder mehrere Netzwerke zu verbinden. Allerdings gelten Router bei der Verwendung in einem VPN und im Zusammenhang mit Tunneling-Protokollen nicht als sehr sicher. Im Gegensatz zu VPN-Gateways, die speziell für diesen Einsatz entwickelt wurden, sind Router nicht dafür ausgelegt, lediglich nur Pakete der zu verarbeitenden Tunneling- oder Security-Protokolle zu verarbeiten. Auf einem Router kann normaler Datenverkehr mit sämtlichen Protokollen übertragen werden, wobei aber normale Paketfilter keinen besonderen Schutz gegen Hacker-Angriffe bieten, d.h. gegen Angriffe von außen auf das Netzwerk; siehe Lipp, VPN, S. 346; Campo/Pohlmann, Virtual Private Networks, S.130/300, die auf die Schwächen von Routern bei einer VPN-Realisierung verweisen, so unter anderem auf fehlende Schutzmaßnahmen. Vgl. zur Definition eines Gateway auch Campo/Pohlmann, Virtual Private Networks, S. 385 („Secure Gateway“). Siehe zur der Einsatzmöglichkeit von Routern außerdem Buckbesch/Köhler, Virtuelle Private Netze, S. 14/15. Das Angebot der Claranet GmbH „ClaraVPN“, abrufbar unter http://www.claranet.de./ipservices/vpn/vpn_ipsec.php (Website vom 30.09.2006), umfasst ebenfalls eine VPN-Verbindung mittels Routern.

Auf diesem Gateway werden die Tunnel terminiert und die Sicherheitseinstellungen und die Benutzerverwaltung konfiguriert,[205] wobei insbesondere die Parameter für die Authentifizierung der Nutzer, die auf Daten des Servers des Unternehmens bzw. Intranets zugreifen wollen, sowie gegebenenfalls für die Datenverschlüsselung festgelegt sind.[206] Hier arbeiten sämtliche Dienste zum Verpacken und Entpacken der Netzwerkprotokolle, der Datenkomprimierung, der Authentifizierung und der Kontrolle der Verbindungsqualität.[207] Von diesem Gateway aus erfolgt die weitere Versendung der Daten ins lokale Netzwerk oder Firmenzentrale.[208]
Eine von dem Gateway gesteuerte Benutzerverwaltung ist bei einem VPN von außerordentlicher Bedeutung, da lediglich ein Zugriff von autorisierten Nutzern auf die Unternehmenszentrale möglich sein darf. Für die Benutzerauthentifizierung gibt es unterschiedliche technische Verfahren, die von einfachen Passwortverfahren bis hin zu digitalen Zertifikaten reichen.[209] Durch diese Sicherheitsfunktionen kann nur über einen solchen Gateway eine Verbindung in das Firmennetzwerk aufgebaut werden.[210]

Dementsprechend kann in dem obigen Bildbeispiel[211] sowohl eine Verbindung von der mittels Gateway gesicherten Zweigstelle bis zur Firmenzentrale als auch umgekehrt aufgebaut werden, wohingegen aus Sicherheitsgründen kein Verbindungsaufbau von der Firmenzentrale ausgehend zu den Rechnern der

[205] Vgl. auch das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 23, wo die Funktionalitäten des VPN-Servers bzw. Gateway (wie der VPN-Server in dieser Arbeit bezeichnet wird) dargestellt sind und ausgeführt wird, dass dort die Parameter für die Datenübertragung festgelegt werden.
[206] Siehe zur Authentifizierung Heibey in: Roßnagel, Handbuch Datenschutzrecht, 4.5 Rn. 98 ff., der definiert, dass es bei der Authentifikation darum geht, mit hinreichender Sicherheit zu erkennen, ob jemand derjenige ist, als der er sich ausgibt (Mensch-Mensch- oder Mensch-Maschine-Authentifikation), oder dasjenige ist, als das es sich ausgibt (Maschine-Maschine-Authentifikation).
[207] Lipp, VPN, S. 289; siehe auch Böhmer (in der 1 Auflage) Virtual Private Networks, S. 133.
[208] Vgl. auch das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 216 mit dem Hinweis, dass das VPN-Gateway den mittels IPSec neu eingefügten IP-Header entfernt, entschlüsselt und die Daten in das lokale Netzwerk sendet. Siehe außerdem Böhmer (in der 1. Auflage) Virtual Private Networks, S. 217/248, der darauf verweist, dass der Weg vom Gateway zum Endgerät unverschlüsselt erfolgt (in diesem Sinne ebenso in der 2. Auflage, S. 225).
[209] Lipp, VPN, S. 56/351.
[210] Siehe auch Davis, IPSec, S. 290 zum Begriff des „Security Gateway“; außerdem Campo/Pohlmann, Virtual Private Networks, S. 123, die darstellen, dass ein VPN-Gateway unterschiedliche Sicherheitsdienste, wie Vertraulichkeit, Datenintegrität, Authentifikation, Zugangskontrolle, Rechteverwaltung, Beweissicherung und Protokollauswertung bieten kann. Dadurch kann unter anderem erreicht werden, dass keine Fremden in der Lage sind, auf Rechnersysteme zuzugreifen.
[211] Siehe S. 44.

Telearbeiter oder externen Nutzer (ohne Gateway) möglich ist.[212]

bb. Management des Gateways

Bei der obigen Darstellung gibt es die Möglichkeit, dass die Firmenzentrale oder die Zweigstelle die Verwaltung und insbesondere Einstellungen der Gateways selbst übernimmt.[213]

Darüber hinaus gibt es die Möglichkeit, dass dieses Management von einem kommerziellen Anbieter in der Form angeboten wird, dass er die Einrichtung, Betrieb und Administration der Gateway und deren Sicherheit übernimmt.[214]

Im Rahmen dieser Arbeit sollen die folgenden drei Möglichkeiten interessieren:[215]

---

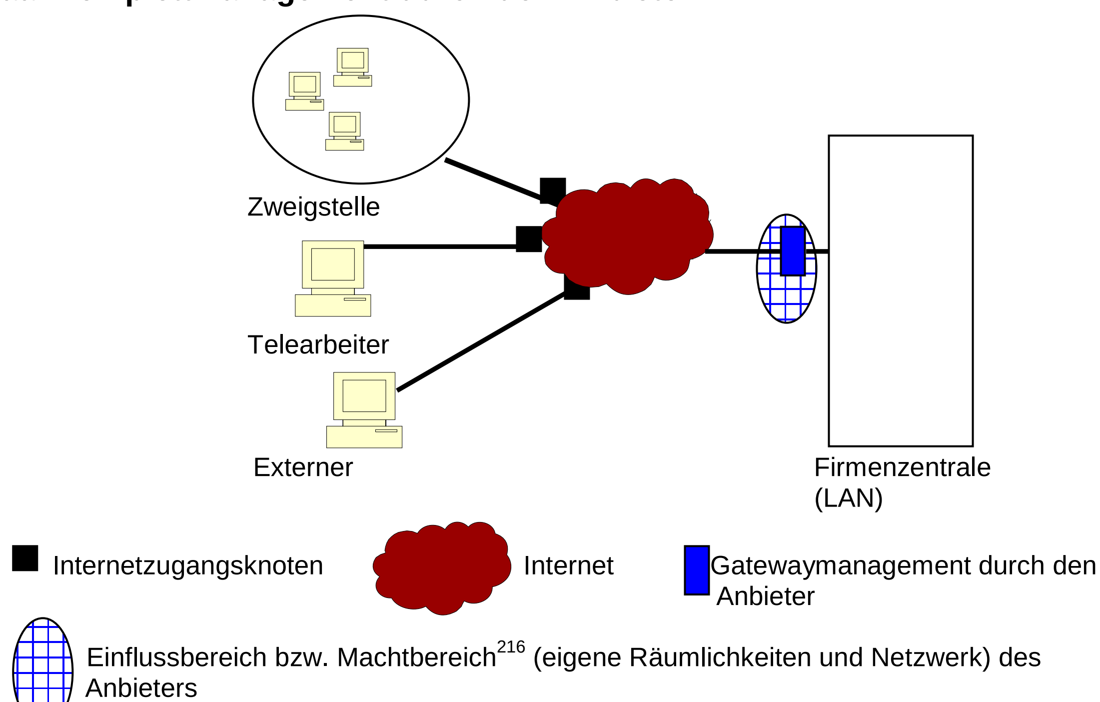
[212] Vgl. Buckbesch/Köhler, Virtuelle Private Netze, S. 16, 21 ff. Hierbei darf jedoch nicht das Missverständnis entstehen, dass eine beiderseitige Kommunikation zwischen Außenstelle und Firmennetz nun vollkommen ausgeschlossen wäre. Über eine bestehende Tunnel-Verbindung können die Anwendungsdaten bidirektional übertragen werden (vgl. Buckbesch/Köhler, Virtuelle Private Netze, S. 23). T-Online („SecureVPN-Benutzerhandbuch", S. 235) bietet zwar darüber hinaus die Möglichkeit eines so genannten Lockrufs an, was bedeutet, dass seitens der Firmenzentrale ein „Ruf" zur Gegenstelle (Clients wie beispielsweise Zweigstelle, Telearbeiter oder Externer) und die Mitteilung erfolgt, dass Daten zum Abruf bereit liegen. Dies darf aber nicht darüber hinwegtäuschen, dass anschließend der Tunnel allein vom Client initiiert werden darf und die Firmenzentrale lediglich den Anstoß zum Tunnelaufbau gibt: Der Gateway der Unternehmenszentrale sendet einen „Lockruf" zum Client und dieser führt anschließend einen Rückruf zum Gateway durch, womit (erst dann) gleichzeitig ein Tunnel aufgebaut wird.

[213] Lipp, VPN, S. 45.

[214] Siehe Lipp, VPN, S. 172/178, der ausführt, dass üblicherweise die Gateways in den Räumen der Endkunden stehen, deren Eigentum sind und auch von ihnen betrieben werden. Jedoch ist auch möglich, dass der Anbieter das VPN als so genannter „Carrier Managed Service" betreibt (so dass die Gateways auch in dessen Räumlichkeiten stehen können). Siehe hierzu auch das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 239, wo so genannte Managed VPNs angeboten werden und eine Weiterleitung der Daten vom Gateway in das Netzwerk des Kunden vorgenommen wird. T-Online weist in seiner Produktbeschreibung darauf hin, dass Einrichtung, Betrieb und Administration der kompletten VPN-Sicherheit von dem Anbieter erbracht wird (aaO). Siehe außerdem Campo/Pohlmann, Virtual Private Networks, S. 124, die ausführen, dass sich der Betrieb hardwarebasierter VPN-Gateways als Service-Geschäftsmodell für Internet Service Provider eignet (siehe außerdem das Beispiel von Campo/Pohlmann, Virtual Private Networks, S. 181/182, in welchem dargestellt ist, dass Netzwerkverwaltung sowie Sicherheitsverwaltung bei einem VPN auf den Anbieter übertragen werden kann. In diesem Sinne auch Buckbesch/Köhler, Virtuelle Private Netze, S. 95. Zum „Managed VPN" siehe außerdem Lienemann, Virtuelle Private Netzwerke, S. 23/24 und Böhmer, Virtual Private Networks (2. Auflage), S. 337. Siehe außerdem zum Begriff des „Managed Services" unter dem Stichwort „Individueller Serverbetrieb" das Angebot von QSC, Applikationsserver innerhalb eines VPN bereitzustellen und zu betreiben (http://www.qsc.de/de/qsc-solutions/managed_services/server/index.html, Website vom 30.09.2006)

[215] Siehe auch Buckbesch/Köhler, Virtuelle Private Netze, S. 113/114 mit dem Hinweis, dass es für den Anwender grundsätzlich diese bzw. die im Folgenden dargestellten Varianten gibt.

aaa. Komplettmanagement durch den Anbieter



Die Übertragung der Daten erfolgt über das Internet bis zu einem Gateway. Der Gateway wird vollständig vom Anbieter gemanaged.[217] Er übernimmt Einrichtung, Betrieb und Administration des Gateways und dessen Sicherheit, so dass davon auch Benutzerverwaltung und Verschlüsselung umfasst sind.[218] Vom Gateway aus erfolgt eine Datenweiterleitung in das lokale Netz (LAN) des Kunden.

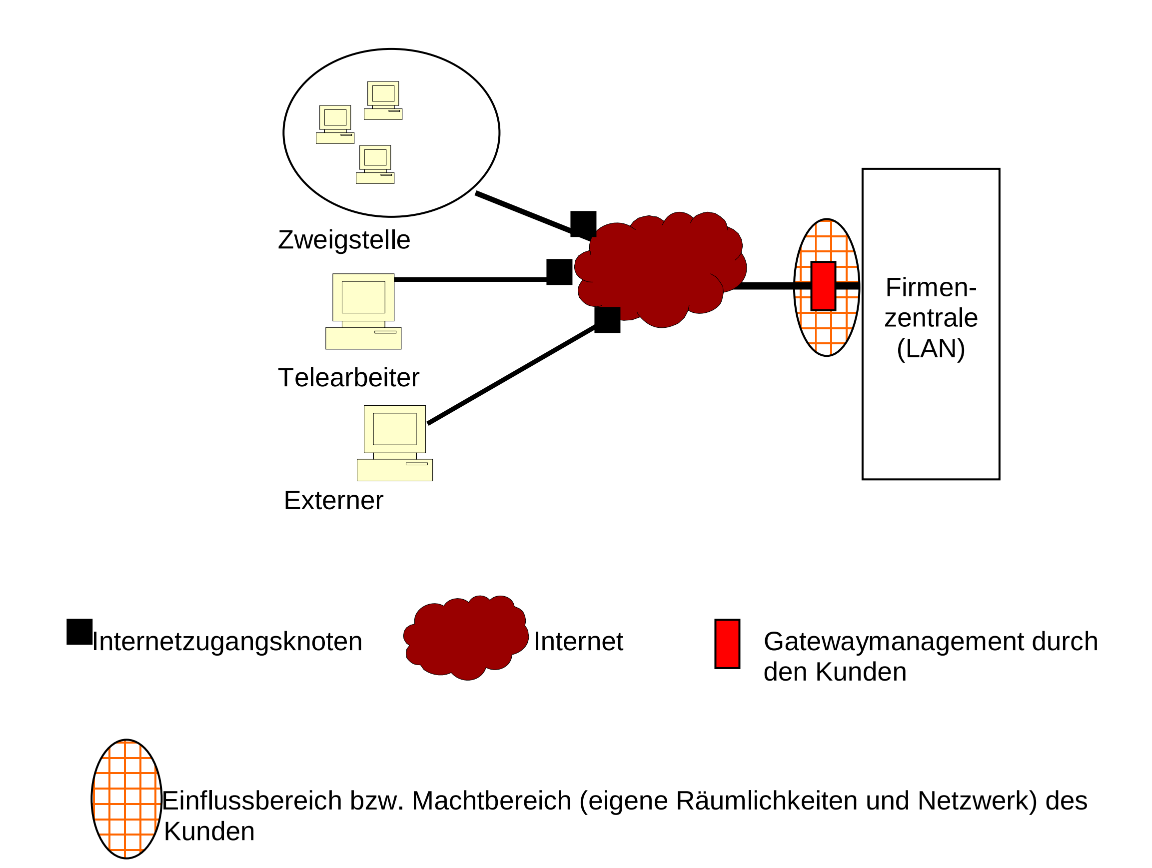
---

[216] Siehe allgemein zum so genannten "Business Process Outsourcing" (BPO) die Ausführungen von Söbbing in: Köhler-Frost, Outsourcing, S. 95 mit dem Hinweis (S.97), dass hier weitreichendere datenschutzrechtliche Anforderungen zu erfüllen sind.

[217] Vgl. hierzu insbesondere das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 239. Dort wird die Bezeichnung „Managed VPN" genutzt, wobei es sich nicht um eine feststehende Definition handelt, da das Systemmanagement mit mehr oder weniger Beteiligung des Anbieters erfolgen kann (siehe auch das Schema bei Böhmer, Virtual Private Networks (2. Auflage), S. 343). Siehe zu dem Begriff des „gemanagten VPN" ebenso Böhmer, Virtual Private Networks (2. Auflage), S. 337 ff. sowie Lienemann, Virtuelle Private Netzwerke, S. 23/24. Siehe außerdem Campo/Pohlmann, Virtual Private Networks, S. 123 mit dem Hinweis, dass sich die Einrichtung und der Betrieb hardwarebasierter VPN-Gateways auch als Geschäftsmodell für den Internet Service Provider eignet. Siehe außerdem zum „Managed VPN-Gateway" das Angebot der Inside Security IT Consulting GmbH unter http://www.inside-security.de/vpn_gateway.html und http://www.inside-security.de/sec_management.html#wartung. Angebote für „Managed VPN" finden sich auch bei VeriSign unter http://www.verisign.de/products-services/security-services/managed-security-services/vpn/index.html sowie auf der Website der interscholz Internet Serivces GmbH & Co. KG (http://www.interscholz.net/produkte/business/14).

[218] Vgl. hierzu etwa das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 239 unter anderem mit dem Hinweis, dass diese Gateways stets über eine feste IP-Adresse verfügen muss. Außerdem Lipp, VPN, S. 46/398, der dieses Modell als vollständiges VPN-Outsourcing bezeichnet, da der vollständige Betrieb vom Anbieter durchgeführt wird, inklusive der Benutzerverwaltung und der Verschlüsselung. Es ist hierbei jedoch nicht notwendig, dass der Anbieter zwangsläufig Eigentümer oder Mieter der Leitungen bzw. der Netze ist (siehe Fn. 93 zur Lizenzpflicht gemäß § 6 TKG a.F. und Meldepflicht gemäß § 6 TKG n.F.), die vom Gateway zum Kundennetzwerk führen. So ist etwa möglich, dass eine ISDN-Verbindung vom Gateway zum Kundennetzwerk besteht, wobei diese Leitung nicht notwendigerweise vom Provider betrieben werden muss. Siehe außerdem zum Begriff des „Security Gateway" Fn. 202.

bbb. Komplettmanagement durch den Kunden



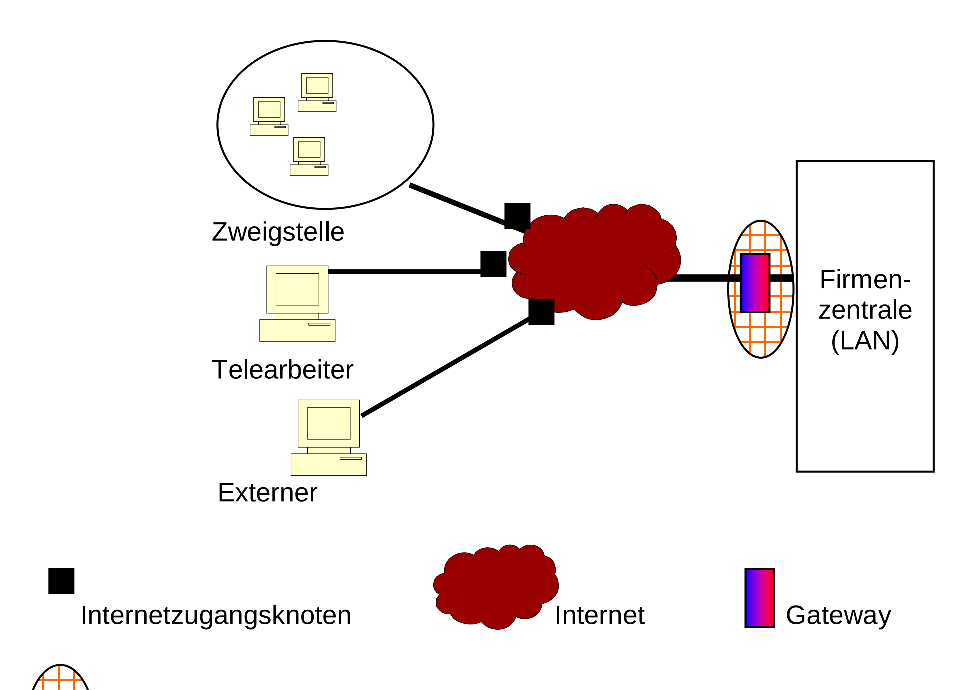
Der Gateway wird vollständig vom Kunden gemanaged.[219] Er übernimmt Einrichtung, Betrieb und Administration des Gateways und dessen Sicherheit, wobei der Gateway in seinem Einflussbereich bzw. Machtbereich steht.
Die Leistung des Anbieters liegt hier in der Bereitstellung des Internetzugangs sowie der Bereitstellung (z.B. Verkauf) der VPN-Technik, etwa der VPN-Hardware und VPN-Software wie beispielsweise IPSec.[220]

[219] Lipp, VPN, S. 45.
[220] Vgl. das Angebot von T-Online „SecureVPN-Benutzerhandbuch".

ccc. Splitmanagement des Gateways[221]

Für die späteren rechtlichen Ausführungen ist entscheidend, wer die Kontrolle über den Gateway innehat, weshalb - wie im folgenden - zwischen den Einflussbereichen von Kunden und Anbieter unterschieden wird.

(1) Splitmanagement im Machtbereich des Kunden



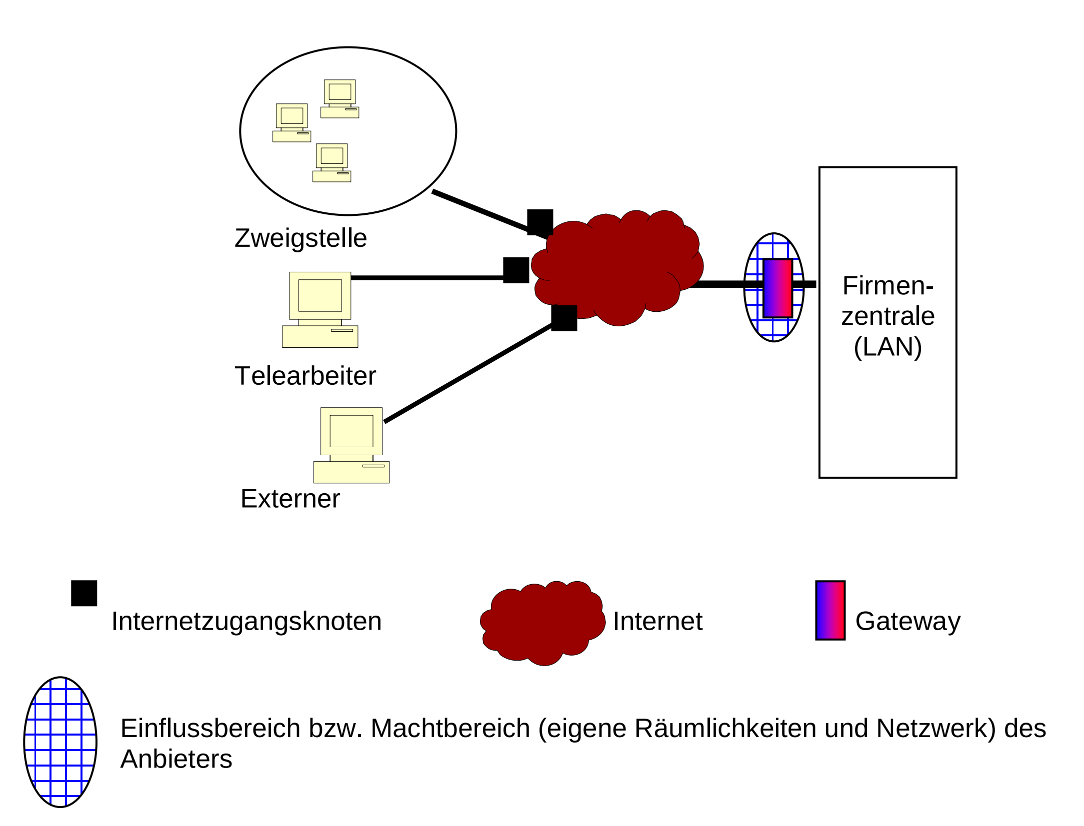
Einflussbereich bzw. Machtbereich (eigene Räumlichkeiten und Netzwerk) des Kunden

Der Gateway wird vom Anbieter in der Form gemanaged, dass er Service-Leistungen und Wartungsarbeiten übernimmt (Servicemanagement).[222] Der Gateway steht jedoch im Einflussbereich bzw. Machtbereich des Kunden, wobei dem Kunden die Vornahme der Sicherheitseinstellungen und Konfiguration der Tunnel und die Benutzerverwaltung obliegt, und er *insoweit* den Gateway managed. Die Funktion des Providers beschränkt sich damit auf die Funktion eines Servicedienstleisters ohne Einfluss auf die eigentlichen sicherheitsrelevanten Funktionen wie Tunnelkonfiguration und Benutzerverwaltung.
Der Anbieter stellt darüber hinaus die Internet-Zugänge an den Standorten zur Verfügung.

---

[221] Vgl. Lipp, VPN, S. 45 und Buckbesch/Köhler, Virtuelle Private Netze, S. 114, die dies als Splitmanagement bzw. geteiltes Gerätemanagement bezeichnen.
[222] Siehe Lipp, VPN, S. 45. Siehe allgemein zum so genannten Infrastrukturvertrag, bei dem der Kunde dem Anbieter den Zugang zu seinen Räumlichkeiten und seiner Infrastruktur gewähren muss, die Ausführungen von Söbbing in: Köhler-Frost, Outsourcing, S. 94.

(2) Splitmanagement im Machtbereich des Anbieters[223]



Die Ausführungen zu Beispiel aaa. gelten entsprechend, der Gateway steht jedoch im Einflussbereich bzw. Machtbereich des Anbieters. Der Kunde kann hier die Administration und Benutzerverwaltung beispielsweise durch Fernzugriff vornehmen. Dieses Beispiel soll ergänzend Berücksichtigung finden, da es grundsätzlich möglich ist, auch die Einstellungen zur Benutzerverwaltung und Sicherheitstechnik, insbesondere Verschlüsselung, durch einen Fernzugriff des Kunden (mittels des Internet) zu ermöglichen - gleichwohl es in der Praxis häufiger vorkommen wird, dass der Kunde in seinem eigenen Machtbereich (durch ein Komplettmanagement) die Benutzerverwaltung und Verschlüsselung vornimmt.[224]

---

[223] Vgl. etwa Buckbesch/Köhler, Virtuelle Private Netze, S. 114, die darstellen, dass der Gateway im Eigentum des Anbieters steht und von diesem kontrolliert wird.

[224] Zur Möglichkeit des Fernzugriffs vgl. Lipp, VPN, S. 335, der in diesem Zusammenhang auch auf die Notwendigkeit des verschlüsselten Zugriffs verweist. Vgl. zur Remote-Administration und zentralen Benutzerverwaltung durch Fernwartungssoftware (allerdings bezogen auf die einzelnen Nutzer) das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 91 ff. Siehe außerdem das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 24 mit dem Hinweis, dass die Konfiguration sämtlicher Systeme (VPN-Gateway) lokal oder remote möglich ist.

b. Software-VPN

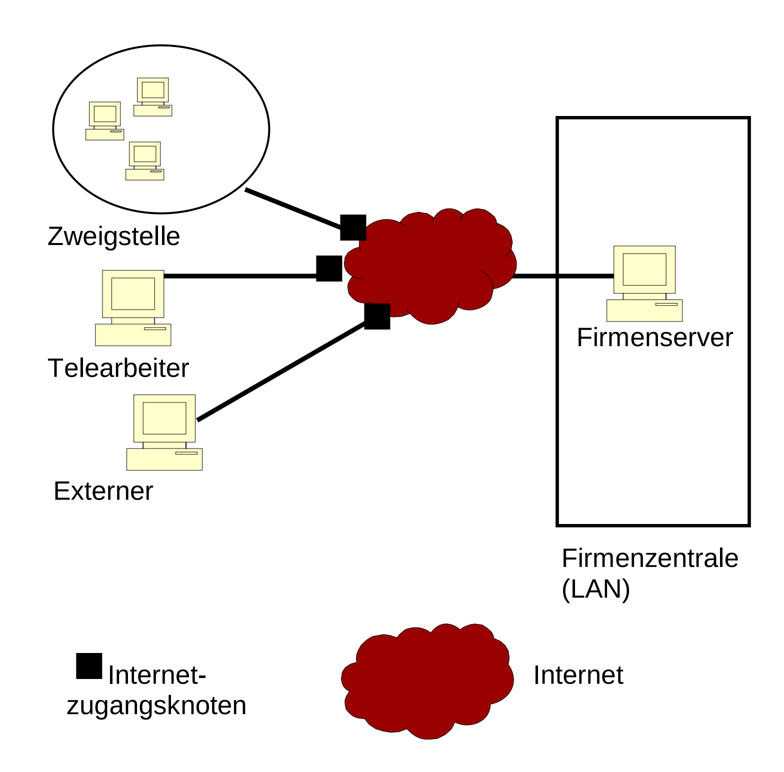
aa. Beispiel

Es gibt außerdem die Möglichkeit, auf den Einsatz eines Gateway zu verzichten und lediglich auf den einzelnen Rechnern, die Zugriff auf das Unternehmensnetz bzw. Firmenzentrale erhalten sollen, spezielle VPN-Software zu installieren.[225]
Hierfür ist erforderlich, dass der Kunde bzw. ein von ihm legitimierter Administrator[226] eine Benutzerverwaltung auf einem Rechner bzw. Server in der Firmenzentrale vornimmt, um sicherzustellen, dass nur berechtigte Nutzer auf das VPN Zugriff erhalten und miteinander kommunizieren können.[227] Ebenso ist der Einsatz von Passwörtern notwendig, allerdings kein Einsatz zusätzlicher Hardware, sprich Gateways.[228]
Dies wird ebenso als End-to-End-Verschlüsselung bezeichnet.[229] So umfasst der Transportmodus von IPSec eine Ende-Zu-Ende-Kommunikation. Allerdings wird der IP-Header nicht verschlüsselt, sondern lediglich der Datenteil.[230]
Es handelt sich um eine rein Software-basierte Lösung, wobei jedoch die Bereitstellung eines Internetzugangs als Grundvoraussetzung vorliegen muss. Auch hier kann eine Verbindung aus Sicherheitsgründen stets nur zu dem Rechner bzw. Server aufgebaut werden, auf welchem die VPN-Software nebst

---

[225] Siehe Fn. 4 und dem dortigen Hinweis auf das Angebot von T-Online abrufbar unter www.t-online.de/directVPN.
[226] Zu der Verwaltung des VPN durch einen Administrator siehe das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch", S. 6/11 ff.
[227] Siehe das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch", S. 3 ff. (Fn. 9) sowie speziell zur Einrichtung der Benutzerverwaltung S. 13 ff. Siehe aber auch Campo/Pohlmann, Virtual Private Networks, S. 124, die darauf aufmerksam machen, dass es gute Gründe für den Einsatz hardwarebasierter VPN-Gateways gibt, da die Verschlüsselung unabhängig vom PC- und Netzwerkbetriebssystem durchgeführt wird und damit die hardwarebasierten VPN nicht die Effektivität des Netzwerks beeinträchtigen. Vgl. auch Böhmer (in der 1. Auflage) Virtual Private Networks, S. 225, der darstellt, dass es sicherheitstechnisch sinnvoll ist, den Gateway aus dem Einflussbereich des lokalen Netzwerkes zu entfernen. In diesem Sinne auch Campo/Pohlmann, Virtual Private Networks, S. 211 und Lipp, VPN, S. 334/335, die auf die erhebliche Bedeutung von zugangsgesicherten und abgeschlossenen Räumlichkeiten bezüglich der VPN-Komponenten verweisen. Dies bedeutet aber im Umkehrschluss, dass es sicherheitstechnisch bedenklich ist, sofern die Sicherheitslösungen eines VPN auf einem Rechner, der im lokalen Netzwerk genutzt wird, installiert sind.
[228] Vgl. auch Campo/Pohlmann, Virtual Private Networks, S. 273 zu den Anforderungen eines Sicherheitskonzepts an einen Gateway (und dem Rat, so wenig wie möglich Software auf diesem Server zu installieren).
[229] Campo/Pohlmann, Virtual Private Networks, S. 124; Abel, Praxishandbuch, IT-Know-how für den Datenschutzbeauftragten, Teil 5/2.3.3 S. 5.
[230] Siehe hierzu die obigen Ausführungen auf S. 43.

Benutzerverwaltung installiert ist.[231] Der (verschlüsselte) Datentunnel besteht zwischen den Rechnern der Nutzer (Telearbeiter, Externer oder Nutzer der Zweigstelle) sowie dem Firmenserver.[232]



Ein Rechner (in der Firmenzentrale) sowie die einzelnen Rechner der Zweigstellen, Telearbeiter und Externen (beispielsweise Lieferanten oder freie Mitarbeiter, die nicht ein Unternehmen eingegliedert sind) haben VPN-Software installiert. Die einzelnen Rechner der Zweigstellen, Telearbeiter und Externen können unter der Voraussetzung, dass eine Online-Verbindung besteht, auf Daten in dem Firmennetzwerk Zugriff nehmen sowie untereinander kommunizieren. Hierbei werden Datentunnel zwischen Rechnern der Nutzer (Zweigstelle, Telearbeiter, Externer) sowie Firmenzentrale aufgebaut.
Der Zugriff auf den Internetzugangsknoten erfolgt auch in diesem Beispiel über das Telefonnetz,[233] was durch Verbindungslinien zwischen Zweigstelle, Telearbeit, Externer sowie dem Internetzugangsknoten dargestellt ist.

---

[231] Vgl. das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch", S. 14, in welchem ausgeführt wird, dass ein Benutzer nach der erfolgreichen Anmeldung am directVPN mit anderen angemeldeten Computern Daten austauschen kann.
[232] Zur Verschlüsselung der VPN-Verbindung mittels IPSec siehe das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch", S. 3.
[233] Siehe zu den anderen Verbindungsmöglichkeiten auch oben Fn. 197.

bb. Systemmanagement

Beim Software-VPN obliegt dem Kunden das Management bzw. die Administration des VPN nebst Benutzerverwaltung. Der Server, auf dem die VPN-Software (inklusive Benutzerverwaltung und Sicherheitseinstellungen) enthalten ist, befindet sich in der Firmenzentrale des Kunden.
Seitens des Providers können sich eigene Managementleistungen beispielsweise auf regelmäßige Wartung oder Fernwartung[234] oder andere Serviceleistungen, wie etwa (automatische Online-) Lieferung von Updates der VPN-Software beziehen.

c. Tunnel-Endpunkte und Tunnel-Startpunkte

Innerhalb eines VPN wird allgemein von Tunnel-Startpunkten und Tunnel-Endpunkten gesprochen.[235]
Als Grundvoraussetzung der Kommunikation sind stets IP-Adressen an diesen Punkten erforderlich.[236]
Bei einem Gateway-VPN ist Tunnel-Endpunkt stets der Gateway des Unternehmens. Dies ergibt sich aus den obigen Ausführungen,[237] wonach in allen Fällen die VPN-Verbindung von Seiten des Client-Rechners in Richtung Firmenzentrale oder zu einem anderen mittels Gateway gesicherten Netzwerk, auf welchen die Tunneling-Funktionen implementiert sind, gestartet werden muss.
Der Gateway muss eine feste bzw. statische IP-Adresse aufweisen.[238] Bei dynamischer Adresszuweisung können die Tunnel-Verbindungen nicht

[234] Siehe zum so genannten „Remote Access“ auch Bischof/Witzel, ITRB 2003, 31, 37.
[235] Vgl. etwa Lipp. VPN, S. 169 ff.; Buckbesch/Köhler, Virtuelle Private Netze, S. 13/17.
[236] Siehe zur IP-Adresse S. 21 ff.
[237] Siehe oben S. 47.
[238] Siehe das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 151, in welchem die IP-Adresse des Gateways als Tunnel-Endpunkt bezeichnet wird, sowie den Hinweis (S. 227), dass der Gateway (als Secure Server bezeichnet) des Unternehmens eine offizielle IP-Adresse benötigt. Siehe zum Erfordernis der festen IP-Adresse des Gateways ebenso Lipp, VPN, S. 176; Davis, IPSec, S. 294; Buckbesch/Köhler, Virtuelle Private Netze, S. 13/17. Dies ändert im Übrigen nichts daran, dass das Zielsystem zur Erleichterung der Anwender und Nutzer zusätzlich zur IP-Adresse einen Domain-Namen erhalten kann (zum DNS-Verfahren siehe S. 30).

konfiguriert werden, weil die Zieladresse unbekannt ist und sich ständig ändert.[239]

Das Erfordernis einer festen IP-Adresse kann allenfalls durch den Einsatz eines so genannten dynamischen DNS-Servers vermieden werden.

Der dynamische DNS-Server beinhaltet ein Verfahren, um Systeme anstatt mit einer festen IP-Adresse über einen Namen ansprechen zu können. Trotz sich ändernder IP-Adresse wird ein Server stets dem korrekten Domain-Namen zugeordnet.[240] Hierfür ist allerdings erforderlich, dass das Unternehmensnetz zumindest dann mit dem Internet verbunden ist, wenn ein Nutzer, beispielsweise ein Telearbeiter, auf die Firmenzentrale zugreifen möchte, da ansonsten ein Verbindungsaufbau nicht möglich wäre.[241] Daher kommt hier die DSL-Technik in Verknüpfung mit einer Flatrate in Betracht, die die Möglichkeit einer zeitlich unbegrenzten Nutzung schafft.[242]

Dementsprechend gilt ebenso bei einem Software-VPN, dass der Rechner in der Firmenzentrale, auf welchem die Benutzerverwaltung und Tunneling-Technik installiert ist, grundsätzlich eine feste IP-Adresse aufweisen müsste.[243] Hier kann jedoch gleichermaßen die Möglichkeit einer dynamischen IP-Adresszuweisung unter der Voraussetzung in Betracht kommen, dass das Firmennetz einen „festen“ Domain-Namen erhält und darüber hinaus die beteiligten VPN-Rechner mit dem Internet verbunden sind.

[239] Buckbesch/Köhler, Virtuelle Private Netze, S. 81; Lipp, VPN, S. 326.

[240] Im Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 236 ff. wird zwar auf die grundsätzliche Notwendigkeit einer festen IP-Adresse hingewiesen, jedoch darüber hinaus ein Verfahren angeboten (so genannter dynamischen DNS-Server), welches unter der Voraussetzung einer stetigen Online-Verbindung auch eine dynamische IP-Adresse des angewählten Standorts zulässt. In diesem Falle wird beim Anbieter auf den von ihm betriebenen dynamischen DNS-Server anstatt einer festen IP-Adresse ein eindeutiger Name des Gateways hinterlegt. Dynamische DNS-Server ermöglichen im Gegensatz zu anderen DNS-Servern (vgl. zum DNS-Verfahren S. 30), die lediglich feste IP-Adressen einem Domain-Namen zuordnen können, auch die Zuweisung von Domain-Namen zu dynamischen (wechselnden) IP-Adressen. Siehe zum Dynamic Domain Name Server auch Lipp, VPN, S. 83 sowie Voss, Das große PC & Internet Lexikon 2007, S. 246(dynamisches DNS).

[241] Vgl. hierzu die vorherige Fn. 240. Da ein Verbindungsaufbau auch hier nur funktionieren kann, sofern die beteiligten Stellen mit dem Internet verbunden sind, bietet T-Online seinen Kunden gleichzeitig einen DSL-Anschluss mit der Möglichkeit der Flatrate an (zur Begriffserklärung einer Flatrate siehe Kroiß/Schuhbeck, Jura Online, S. 7). Bei einer Flatrate wird eine dynamische IP-Adresse zugewiesen, die sich in der Regel spätestens nach 24 Stunden ändert (Voss, Das große PC & Internet Lexikon 2007, S. 351).

[242] Siehe zur Flatrate auch S. 29.

[243] Vgl. auch S. 53 ff. zu den Sicherheitsanforderungen eines Software-VPN.

Tunnel-Startpunkte sind sowohl bei einem Gateway-VPN als auch bei einem Software-VPN die (Rechner der) Zweigstellen, Telearbeiter und Externen, wobei bei diesen grundsätzlich gleichgültig ist, ob diese dynamische oder feste IP-Adressen aufweisen.[244] Bei einem Gateway-VPN kann damit ebenso ein Rechner oder Gateway der Firmenzentrale Tunnel-Startpunkt sein.[245] Dementsprechend können sich bei einem Gateway-VPN oder Software-VPN aber ebenfalls Telearbeitsplätze im häuslichen Bereich oder kleine Außenstellen, für welche sich die Anschaffung eines Gateways mit statischer IP-Adresse unter Umständen finanziell nicht lohnt,[246] in das Unternehmensnetz einwählen.[247]

3. Freiwilliges und zwangsweises Tunneling

a. Zwangsweises Tunneling

Zwangsweises Tunneling bedeutet, dass ein Nutzer bzw. Client,[248] der sich in das Internet einwählt, stets nur zu einem vordefinierten Unternehmensstandort weitergeleitet wird, und nicht selbst entscheiden kann, ob ein Tunnel aufgebaut wird.[249]

Der jeweilige Anbieter des Internetzugangs schafft regelmäßig an seinem Internetzugangsknoten (PoP bzw. Einwahlserver oder Vermittlungsstelle)[250] oder auf einer Datenbank, auf welche der Internetzugangsknoten Zugriff nimmt, und die die notwendigen Parameter für die Datenweiterleitung enthält,

---

[244] Lipp, VPN, S. 177/265/326. Mindestvoraussetzung der Kommunikation ist eine dynamische IP-Adresse.

[245] Siehe das obige Beispiel auf S. 44. Aus Sicherheitsgründen muss allerdings eine Verbindung zu einer (anderen) mittels Gateway gesicherten Stelle aufgebaut werden.

[246] Nicht nur der Erwerb zusätzlicher Hardware bedeutet zusätzliche Kosten, sondern auch statische IP-Adressen, die sich Anbieter –aufgrund ihrer Knappheit – oftmals sehr teuer bezahlen lassen (vgl. etwa Lipp, VPN, S. 177).

[247] Tunnel-Startpunkt kann unter Umständen ebenso der PoP des Anbieters sein. Siehe hierzu Lipp, VPN, S. 178/289, der darauf verweist, dass in die PoPs spezielle Funktionen implementiert werden müssen, um entsprechende Tunnel aufbauen zu können (siehe außerdem die nachfolgenden Ausführungen zum zwangsweisen Tunneling).

[248] In den obigen Beispielen (Gateway-VPN und Software-VPN) sind Clients etwa die Telearbeiter, Externe oder Mitarbeiter innerhalb einer Zweigstelle. Zum Begriff des Client-Server-Prinzips siehe außerdem die Ausführungen auf S. 43.

[249] Lipp, VPN, S. 178/292; Buckbesch/Köhler, Virtuelle Private Netze, S. 15/16. Siehe auch zur Erklärung des zwangsweisen Tunneling auch S. 12 des Whitepaper von Microsoft (http://download.microsoft.com/download/f/3/c/f3c3a5f6-cb26-4188-a23f-278106e32566/vpnoverview.pdf - Website vom 30.09.2006).

[250] Siehe hierzu S. 29.

die Voraussetzungen für die Weiterleitung in die Firmenzentrale.[251] Teilweise werden zu diesem Zwecke – ebenso wie im Rahmen des Internet-Access- so genannte RADIUS-Server eingesetzt,[252] wobei zum zusätzlichen Schutz der ausgetauschten Benutzerkennung und des Passwortes eine symmetrische Verschlüsselung eingesetzt werden kann.[253] Diesen vordefinierten Tunnel („compulsary Tunnel“) durch das Internet kann das PC-Endgerät bzw. der Nutzer nicht verlassen, da er statische Eigenschaften aufweist.[254] Der Nutzer hat keinen Einfluss auf den Aufbau des Tunnels.

Voraussetzung für dieses Modell des zwangsweisen Tunneling ist der Einsatz des oben behandelten Protokolls L2TP.[255] Auch beim zwangsweisen Tunneling ist daher eine zusätzliche Datenverschlüsselung erforderlich, etwa durch die Verwendung des Tunneling-Protokolls IPSec,[256] wobei diese Verschachtelung von L2TP und IPSec –zumindest zurzeit - auf dem Markt nur von wenigen Dienstanbietern angeboten wird.[257]

---

[251] Siehe auch Lipp, VPN, S. 285/289, der darauf hinweist, dass die für das zwangsweise Tunneling erforderlichen Funktionalitäten meist auf den PoPs der Service Provider und/oder Carriern (Netzeigentümern) bzw. auf einer Datenbank, auf die der PoP Zugriff nimmt, implementiert sind (vgl. insgesamt Lipp, VPN, S. 178/292/305 ff.).

[252] Siehe zur Funktion des Radius-Servers S. 29. Lienemann, Virtuelle Private Netzwerke, S.119 führt zum zwangsweisen Tunneling aus, dass die Authentifizierung meist auf dem RADIUS-Server stattfindet.

[253] Böhmer, Virtual Private Networks, S. 200 (in der ersten Auflage).

[254] Böhmer, Virtual Private Networks (2. Auflage), S. 216. Siehe hierzu auch Buckbesch/Köhler, Virtuelle Private Netze, S. 103 ff., die an einem Beispiel ausführen, dass in der Datenbank des Servers zu jedem Nutzer fixiert werden kann, auf welchen Tunnel-Endpunkt dieser zu leiten ist, womit automatisch ein weitergehender Tunnel zum Endpunkt aufgebaut wird. Der Nutzer hat hierbei keinen Einfluss darauf, zu welchem Endpunkt er weiterverbunden wird (Buckbesch/Köhler, Virtuelle Private Netze, S. 105).

[255] Lienemann, Virtuelle Private Netzwerke, S. 118; Lipp, VPN, S. 178.

[256] Siehe Lipp, VPN, S. 182; Buckbesch/Köhler, Virtuelle Private Netze, S. 105. L2TP (siehe zu diesem Protokoll S. 35) ist ein Protokoll, welches das zwangsweise Tunneling ermöglicht, hat hingegen keine eigenen Sicherheitsmechanismen (siehe Lipp, VPN, S. 182, der darauf verweist, dass L2TP kein Sicherheitsprotokoll ist). IPSec, welches Datenverschlüsselung beinhaltet, erfordert allerdings, dass der Client selbständig entscheidet, von welchem Startpunkt und zu welchem Endpunkt ein Tunnel aufgebaut werden soll, da nur in diesem Falle die Verschlüsselung zwischen Client und Firmenzentrale erreicht werden kann (vgl. Lipp, VPN, S. 182). Daher kommt eine so genannte Verschachtelung von IPSec und L2TP in Betracht (Lipp, VPN, S. 182) mit der Folge, dass zwischen Client (etwa dem Mitarbeiter einer Zweigstelle, Telearbeiter oder Externen) und Firmenzentrale eine verschlüsselte Verbindung besteht, aber dennoch der Client mittels L2TP zwangsweise zur Firmenzentrale getunnelt wird. Anderenfalls beginnt der Tunnel erst im PoP des Providers, so dass der PoP damit Tunnel-Startpunkt ist, wobei in diesem Falle allein mittels L2TP ausschließlich ein unverschlüsselter Tunnel zwischen PoP und Firmenzentrale aufgebaut wird, sofern nicht der Anbieter des Internetzugangs die Verschlüsselung für den Kunden vornimmt. Diese Variante wird auch als Enterprise-Modell bezeichnet (vgl. Lipp, S. 171).

[257] Lipp, VPN, S. 186. Siehe aber zu dieser Möglichkeit das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 226.

Der Internetzugangspunkt bzw. die nachgeschaltete Datenbank oder RADIUS-Server übernimmt beim zwangsweisen Tunneling einen Teil der Benutzerauthentifizierung im VPN, wobei die weitere Identifizierung im Gateway stattfindet.[258]
Diese Authentifizierung kann dadurch erfolgen, dass jedem Kunden eine lediglich einmal vergebene Einwahlnummer zugewiesen wird, mit der er sich bzw. die von ihm legitimierten Nutzer, insbesondere seine Mitarbeiter, bei dem Anbieter des Internetzugangs einwählt, und anhand derer dem Anbieter sofort bekannt ist, dass ein Tunnel zum Unternehmen XY aufzubauen ist.[259]

Eine weitere Möglichkeit besteht darin, dem einzelnen Nutzer eine Kennung zu geben, mit welcher er sich in das Netz des Anbieters einwählt, und anhand derer der Anbieter die Zuordnung zu einem Unternehmen vornimmt.[260]
Bei der Benutzerkennung kann es sich gegebenenfalls um Eigennamen der Nutzer, Passwörter oder Zertifizierungsverfahren/Zertifikate handeln.[261]
Ein Teil der Benutzerauthentifizierung kann beispielsweise durch Vor- und Nachname des einzelnen Nutzers festgelegt werden, die dem Anbieter bekannt gegeben werden und die er stets einem Unternehmen zuordnet. Wählt sich beispielsweise ein „Martin Müller“ aus dem Unternehmen X in das Netz des Anbieters ein, kann der Anbieter mittels einer vorangegangen Speicherung dieser Identifikationsmerkmale an seinem Internetzugangspunkt bzw. in einer Datenbank, auf die der Internetzugangspunkt Zugriff nimmt, die Zuordnung zwischen Martin Müller und dem Unternehmen X vornehmen.
Dies erfolgt entweder durch ein so genanntes Präfix (vorangestellte Kennung) oder Suffix (angehängte Kennung), so dass die Zuordnung in der Datenbank des Anbieters beispielsweise martin.mueller@Unternehmen-X lautet.[262]
Darüber hinaus kann sich der Nutzer zusätzlich durch Passwörter und/oder digitalen Zertifikaten[263] authentifizieren.

[258] Siehe Lipp, VPN, S. 286 ff.
[259] Lipp, VPN, S. 287/288/292; vgl. zur Einwahlnummer auch Buckbesch/Köhler, Virtuelle Private Netze, S. 15/16.
[260] Lipp, VPN, S. 287; Buckbesch/Köhler, Virtuelle Private Netze, S. 16.
[261] Lipp, VPN, S. 56, 145 ff.
[262] Lipp, VPN, S. 287.
[263] Siehe zu digitalen Signaturen und digitalen Zertifikaten die Ausführungen von Lipp, VPN, S. 150 ff.

Außerdem ist es seitens des Anbieters ebenso möglich, den Nutzern als Benutzernamen unterschiedliche Ziffernkombinationen bereit zu stellen, welche diese bei Einwahl ins Netz angeben müssen.[264]
So ist dementsprechend ebenso eine Authentifizierungsmethode durchführbar, nach welcher dem Anbieter die Nutzer nicht zwangsläufig namensmäßig bekannt gegeben werden müssen, sondern der Anbieter seinem Vertragspartner bzw. Kunden mehrere (ziffernmäßige) Benutzernamen bereitstellt, dieser anschließend an seine Nutzer in eigenständiger Verwaltung weitergibt. [265]

b. Freiwilliges Tunneling

Freiwilliges Tunneling bedeutet hingegen, dass der jeweilige Nutzer selbst entscheiden kann, ob und wohin ein Tunnel aufgebaut werden soll oder nicht.[266]
Der Anbieter des Internetzugangs nimmt keine Benutzerauthentifizierung für den VPN-Zugang vor.
Möchte der jeweilige Nutzer also auf das Unternehmensnetz zugreifen, findet seine Identifizierung allein im entsprechenden Gateway statt.[267]
Der Tunnel wird von Rechner zu Gateway aufgebaut und nicht wie beim oben beschriebenen zwangsweisen Tunneling seitens des Diensteanbieters zum Unternehmens-Gateway.[268] Der Anbieter eines Internetzugangs ist an der Authentifizierung somit nicht beteiligt, sondern übermittelt nur die entsprechenden IP-Pakete.

---

[264] Vgl. zu dieser Identifikationsmethode das Angebot von T-Online „SecureVPN-Benutzerhandbuch". S. 120.

[265] Pasword Authentication Protocol (PAP) hat den Nachteil, dass Passwörter auf Nutzer- und Serverseite in Datenbanken abgelegt werden (siehe Böhmer (in der 1. Auflage) Virtual Private Networks, S. 197). Böhmer führt dazu aus, dass zusätzlichen Schutz der Einsatz des oben angesprochenen RADIUS-Servers bieten kann, sofern zum Schutz der ausgetauschten Nutzer-Kennung und des Passworts eine symmetrische Verschlüsselung eingesetzt wird (Böhmer, Virtual Private Networks (1. Auflage), S. 200). Ausführungen von Böhmer zu PAP finden sich außerdem auf S. 164 ff. in der 2. Auflage, Virtual Private Networks.

[266] Lipp, VPN, S. 179/292/293.

[267] Lipp, VPN, S. 182 verweist in diesem Zusammenhang darauf, dass bei freiwilligem Tunneling ebenso die Möglichkeit besteht, dass der Nutzer sich in das Netz des Anbieters einwählt, ohne die IPSec-Funktionen bzw. Sicherheitsfunktionen zu benutzen, was jedoch der Sicherheitsstrategie des jeweiligen Unternehmens zuwiderlaufen könnte. Aus diesem Grunde gibt es die Möglichkeit, IPSec und L2TP kombiniert anzuwenden, denn dann sei sichergestellt, dass zwangsläufig ein Tunnel aufgebaut wird (siehe zu letzterem die Ausführungen unter Fn. 256).

[268] Diese Variante wird regelmäßig als Ende-zu-Ende-Modell bezeichnet, vgl. auch Lipp, VPN, S. 179/ 182/326.

Entsprechendes gilt bei einem Software-VPN, bei welchem die Authentifizierung allein an dem jeweiligen Rechner bzw. Server stattfindet, welcher die Benutzerverwaltung vornimmt.
Hier darf jedoch nicht das Missverständnis entstehen, dass der Diensteanbieter beim freiwilligen Tunneling überhaupt keine Identifizierung vornimmt. Der Diensteanbieter muss für den berechtigten Netzzugang bzw. Internetzugang stets am RADIUS-Server überprüfen, ob die Benutzerkennung mit der dort gespeicherten Kundenkennung und dem dazugehörigen Passwort übereinstimmt. Bei erfolgreicher Authentifizierung vergibt der RADIUS-Server eine IP-Adresse und ermöglicht dem Nutzer den Zugang in das Internet.

Beim freiwilligen Tunneling können im Übrigen mehrere Tunneling-Protokolle in Betracht kommen. Bei einem Software-VPN wird regelmäßig ausschließlich IPSec verwendet, wohingegen bei einem Gateway-VPN insbesondere das oben beschriebene Protokoll L2TP, IPSec oder L2Sec eingesetzt wird sowie außerdem eine Verschachtelung von L2TP und IPSec möglich ist.[269]
Die Verschachtelung von L2TP sowie IPSec kommt in Frage, da L2TP zum einen keine Datenverschlüsselung ermöglicht. Zum anderen müssen Sicherheitslücken vermieden werden, wenn im Rahmen eines Gateway-VPN der Tunnel-Startpunkt eine dynamische IP-Adresse innehat. So beinhaltet das Standardverfahren zum Schlüsselaustausch bei IPSec (IKE)[270] als ein wesentliches Authentifizierungsprinzip,[271] die eindeutige Identifizierung des Nutzers mittels seiner IP-Adresse.[272] Dies ist jedoch bei dynamisch vergebenen IP-Adressen, etwa bei Telearbeitsplätzen im häuslichen Bereich, problematisch, da hier die jeweiligen Nutzer bei jeder erneuten Einwahl eine andere IP-Adresse zugewiesen bekommen und daher keine Identifizierung möglich wäre.[273] Dieses Defizit kann durch die Verschachtelung von L2TP mit IPSec vermieden werden. So wird hier zunächst ein „fester“ Tunnel zwischen Nutzer und Gateway mittels L2TP aufgebaut und erst im Anschluss die

[269] Siehe auch das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 226 ff.
[270] Siehe zu dem Schlüsselaustausch-Verfahren „IKE“ S. 42.
[271] Siehe hierzu und zu den drei anderen Möglichkeiten der Authentifizierung im Rahmen von IKE Lienemann, Virtuelle Private Netzwerke, S. 112. Siehe auch das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 224 ff.
[272] Lienemann, Virtuelle Private Netzwerke, S. 113.
[273] Vgl. zu dieser Problematik auch Lipp, VPN, S. 177.

Verschlüsselung mittels IPSec und der damit verbundene Schlüsselaustausch vorgenommen, so dass der Nutzer durch den bereits aufgebauten Tunnel nun (für die Verwendung von IPSec) identifizierbar ist.[274]

III. Zusatzdienst E-Mail

1. Protokolle der E-Mail-Kommunikation

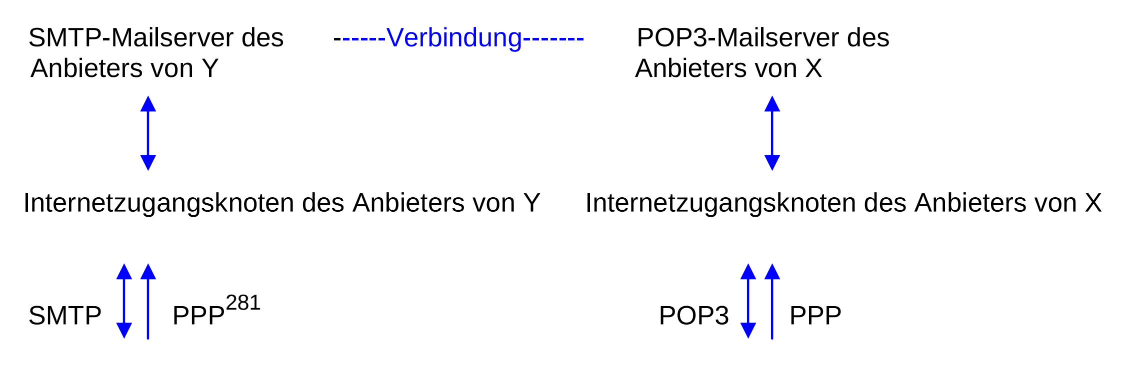
Im Rahmen der E-Mail-Kommunikation gibt es zwei wesentliche Protokolle, um eine Datenübermittlung sicherzustellen:[275]
Mittels des Post Office Protocol 3 (POP 3) können E-Mails vom Empfänger einer solchen vom Server (POP3-Server) des Anbieters, bei dem der Empfänger seinen E-Mail-Account beauftragt hat abgerufen werden. Sie werden dort zwischen gespeichert.[276] Mittlerweile wird, allerdings noch von wenigen Anbietern, ebenso das IMAP (Internet Message Access Protocol) angeboten.[277] IMAP ermöglicht den Nutzern, E-Mails unmittelbar auf dem Server des Providers zu bearbeiten und dort zu speichern.[278]

Der Absender einer E-Mail benutzt regelmäßig das Simple Mail Transfer Protocol (SMTP), um seine E-Mails versenden zu können.[279] Bei diesem Versendungsvorgang wird die E-Mail auf dem E-Mail-(SMTP-)Server des Anbieters, bei welchem der Absender seinen E-Mail-Account beauftragt hat (z.B. t-online, gmx, etc.), zwischengespeichert und von dort zu dem POP3-Server des Empfängers bzw. des Anbieters, bei welchem der Empfänger seinen E-Mail-Account innehat, weitergeleitet.[280]

---

[274] Siehe auch das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 217, S. 224 ff, hier insbesondere S. 226.
[275] Siehe S. 3, wo angesprochen worden, dass die Bereitstellung der E-Mail-Kommunikation regelmäßig eine weitere Teilleistung des VPN-Anbieters darstellt, so dass es notwendig ist, die Funktionsweise darzustellen.
[276] Siehe auch Hobert, Datenschutz und Datensicherheit im Internet, S.229; Cichon, Internetverträge,Rn. 122; teia (Hrsg.), Recht im Internet, S. 34 ff.;
[277] Vgl. zu „IMAP“ Voss, Das große PC & Internet Lexikon 2007, S. 434 ff.; Koch, Internet-Recht, S. 30.
[278] Vgl. ebenso Tanenbaum, Computernetzwerke, S. 661 ff.
[279] Siehe auch Schaar, Datenschutz im Internet, Rn. 12; Sieber in: Hoeren/Sieber, Teil 1 Rn. 114 ff.; Cichon, Internetverträge Rn. 28; teia (Hrsg.), Recht im Internet, S. 34 ff.; Hobert, Datenschutz und Datensicherheit im Internet, S. 40.
[280] Siehe auch die Ausführungen und das Schaubild bei Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 55/56. Vgl. außerdem Tanenbaum, Computernetzwerke, S. 655 ff..

2. Bildbeispiel E-Mail



Sofern der Client bzw. der Absender den gleichen Anbieter haben, können in dem obigen Beispiel auch die Anbieter des E-Mail-Service von Y und Z in einer Person zusammenfallen. Dennoch ist zur Erfüllung der unterschiedlichen Aufgaben im Rahmen der E-Mail-Kommunikation der Einsatz von zwei unterschiedlichen Mailserversystemen erforderlich.

[281] Zu PPP siehe S. 21.

B. Materielle Grundlagen

Im Folgenden werden die materiellen Grundlagen dargestellt, die für die anschließende rechtliche Prüfung relevant sind.
Dies umfasst zum einen die Neudefinition des Begriffs der „Online-Dienste“. Zum anderen werden die einschlägigen Datenschutzgesetze vorgestellt und die Personen charakterisiert, die bei der Bereitstellung eines Online-Dienstes involviert sind. Es werden außerdem die datenschutzrechtlichen Pflichten eines Diensteanbieters erläutert, wobei die Ausführungen ebenso berücksichtigen, inwieweit Datenschutz durch staatliche Überwachungs- und Auskunftspflichten eingeschränkt sein kann.

I. Definition „Online-Dienste“

Ziel dieser Arbeit ist es, dass in der Einführung[282] angesprochene Beziehungsgeflecht umfassend zu prüfen, um die „datenschutzrechtlichen“ Verantwortlichkeiten der beteiligten Personen in einem VPN untereinander und voneinander abgrenzen zu können.
Hierfür ist erforderlich, den Begriff „Online-Dienst“ in Abweichung von seinem gebräuchlichen Begriffsverständnis zu verwenden.

1. Gebräuchliche Begriffsbestimmung

Der Begriff „Online-Dienst“ wird regelmäßig als Synonym für Online-Dienste-Anbieter verwendet wird, womit allein die großen, kommerziellen Anbieter von Informationen und Daten gemeint sind.[283] Hierbei werden etwa T-Online, AOL, Compuserve und MSN als Online-Dienste benannt,[284] die so genannte proprietäre Dienstleistungen zur Verfügung stellen sollen.[285]

---

[282] Siehe S. 5.

[283] Beck-IuKDG-Engel-Flechsig, Glossar „Online-Dienst-Anbieter“, S. 830; Schaar, Datenschutz im Internet, Rn. 304;; Eichhorn, Internet-Recht, S. 42; Koch, Internet-Recht, S. 4; Hobert, Datenschutz und Datensicherheit im Internet, S. 38, 39; Kröger/Kuner, Internet für Juristen, S. 6; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 12. Vgl. auch Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 10/28; Stögmüller in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 68. Siehe auch die nachfolgende Fn. 284

[284] Vgl. insbesondere Wanckel, Persönlichkeitsschutz in der Informationsgesellschaft, S. 64/64, insbesondere dort Fn. 185, dass die Bezeichnung „Online-Dienste“ für kommerzielle Anbieter,

So wird beispielsweise die Aussage getroffen, dass Online-Dienste eigene geschlossene und zentral strukturierte Netze betreiben, die nur ihren registrierten Nutzern offen stehen,[286] und dass es sich bei Online-Diensten um Internet-Provider handelt, die als große kommerzielle Anbieter von Informationen und Daten in ihrem eigenen Netz Angebote bereitstellen, die nur von den Mitgliedern des jeweiligen Dienstes abgerufen werden können.[287]

Dem Verständnis eines Online-Dienstes ist dabei außerdem immanent, dass mehrere Dienstleistungen innerhalb eines Gesamtangebotes vereint sind und es sich um ein kombiniertes[288] Angebot bzw. um ein „Bündel von Leistungen“[289] eines (einzigen) Anbieters als Komplettpaket[290] handelt. Dabei wird regelmäßig auch das Angebot des Internetzugangs verlangt.[291]

---

die über ihre Netze eigene Angebote bereithalten und verschiedene Kommunikations- und Informationsdienstleistungen anbieten (beispielsweise T-Online, AOL, Compuserve und MSN), gebräuchlich geworden ist. Siehe außerdem OLG Hamburg, CR 2000, 363, 363; OLG Hamburg, CR 2000, 522, 522; Eichhorn, Internet-Recht, S. 36; Kröger/Kuner, Internet für Juristen, S. 6; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 12; Ritz, Inhalteverantwortlichkeit von Online-Diensten, S. 14/20; Eberle in: Eberle/Rudolf/Wasserburg, Kapitel Rn. 50; Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 96; Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 9. Siehe auch Cichon, Internetverträge, Rn. 3 (ebenso Fn. 8), die unter Online-Diensten ausschließlich Unternehmen versteht, die ein eigenes Computernetzwerk betreiben, das in aller Regel an das Internet angeschlossen ist. Cichon führt weiter aus, dass dieses Teilnetz auch als proprietäres Netz bezeichnet wird, da die Online-Dienste über dieses Teilnetz im Gegensatz zum Internet die rechtliche und tatsächliche Verfügungsgewalt innehaben, es ihnen also „gehöre“ (Cichon, Internetverträge, Rn. 3 Fn. 8), und Online-Dienste außerdem im Gegensatz zu Access-Providern ihren Kunden nicht nur (via dieses eigenen Netzwerkes) einen Zugang zum Internet zur Verfügung stellen, sondern ihnen darüber hinaus innerhalb des nach außen hin abgeschlossenen Systems zusätzliche Inhalte (Informationen, Chats, Online-Banking, Online-Shopping) anbieten, die für normale Internet-Surfer nicht zugänglich sind.

[285] Siehe zum Begriff „proprietär“ auch Voss, Das große PC & Internet Lexikon 2007, S. 663, der den Begriff „proprietär“ Eigenschaften zuordnet, die einem bestimmten Eigentümer gehören bzw. eigen sind. Siehe auch Wanckel, Persönlichkeitsschutz in der Informationsgesellschaft, S. 63/64/66, der zwar einerseits Content-Provider und Access-Provider (letztere bezeichnet er als Service-Provider) als Online-Dienste einordnet, andererseits aber davon ausgeht, Online-Dienste ihre Angebote nur ihren Mitgliedern zur Verfügung stellen. Außerdem Cichon, Internetverträge, Rn. 3 Fn. 8 (vgl. vorherige Fn. 284).

[286] Vgl. hierzu Schneider, Verträge über Internet-Access, S. 98.

[287] In diesem Sinne ebenso Kirsten in: Hoeren/Sieber, Teil 10 Rn. 24; Ritz, Inhalteverantwortlichkeit von Online-Diensten, S. 30.

[288] Vgl. Schuster in: TKG-Kommentar (2. Auflage), § 4 TKG Rn. 4a, der ebenso den Begriff „integriertes“ Angebot verwendet. Siehe zum Begriff Kombinationspaket Gersdorf in: TKG-Kommentar (3. Auflage), Einleitung C Rn. 23.

[289] Beck-IuKDG-Engel-Flechsig, Glossar „Online-Dienst-Anbieter“, S. 830; Beck-IuKDG-Tettenborn, § 2 TDG Rn. 43; Eichhorn, Internet-Recht, S. 45; Schneider, Verträge über Internet-Access, S. 93/98; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 12. Zum Begriff des „Allround-Online-Dienstes“ siehe Schaar, Datenschutz im Internet, Rn. 19.

[290] Siehe hierzu S. 4. Siehe auch Lammich in: Moritz, Rechts-Handbuch zum E-Commerce, B Rn.245, der T-Online als Gesamtdienst bzw. Komplettpaket bezeichnet.

[291] Schaar, Datenschutz im Internet, Rn. 19, 304; Koch, Internet-Recht, S. 4; Kröger/Kuner, Internet für Juristen, S. 6; Schneider, Verträge über Internet-Access, S. 93; Wildemann,

Dieses Komplettpaket ist im Sinne der funktionalen[292] Betrachtungsweise in seine einzelnen Leistungsbestandteile und in eine Transport- bzw. Telekommunikationsebene[293] und eine Inhaltsebene zu zerlegen, so dass jedes Angebot eigenständig bestimmt werden kann.[294]

Vertragsschluss im Netz, S. 3; Dilger, Verbraucherschutz bei Vertragsabschlüssen im Internet, S. 12; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 12; Martens/Schwarz-Gondek in: Bräutigam/Leupold, Glossar S. 1084.

[292] Siehe zur funktionalen Betrachtungsweise Pankoke, Von der Presse- zur Providerhaftung, S. 30. Auf die von Waldenberger vertretene Gesamtbetrachtungslehre (siehe Waldenberger, MMR 1998, 124, 125, zustimmend noch Moos in: Kröger/Gimmy, Handbuch zum Internet-Recht (1. Auflage), S. 52/53), die im Wege einer wertenden Gesamtschau auf eine komplexe Internet-Dienstleistung, die aus mehreren (Teil-) Angeboten besteht, lediglich das TDG oder den MDStV anwendet, ist nicht näher einzugehen, da sowohl Rechtsprechung als auch Literatur auf die Zielsetzung eines konkreten Angebots (funktionsbezogene Betrachtungsweise) und nicht auf das Gesamtspektrum der Angebote eines Diensteanbieters abstellen. Vgl. hierzu etwa OLG Hamburg, CR 2000, 363, 363; VG Düsseldorf, AfP 1998, 543 ff. (wobei letztendlich offengelassen wurde, ob es sich bei dem konkreten Angebot um ein journalistisch-redaktionell gestaltetes Angebot handelt, da von vorneherein die Glaubhaftmachung eines den Erlass einer einstweiligen Anordnung erfordernden Anordnungsgrundes fehlte); VG Berlin, K&R 1999, 381, 382 (bestätigt durch OVG Berlin, MMR 1999, 493, 494), wo trotz optischer Dominanz des Rundfunkprogramms die so genannte Laufbandwerbung als Mediendienst qualifiziert wurde. Siehe auch Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2982; v.Bonin/Köster, ZUM 1997, 821, 822; Kröger/Moos, ZUM 1997, 462, 465 ff., insbesondere S. 468.; Gounalakis/Rhode, CR 1998, 487, 489; Kuch, ZUM 1997, 225, 226 ff.; Engel-Flechsig, ZUM 1997, 231 ff. (insbesondere S. 234/238); Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 101; Tettenborn, MMR 1999, 516, 518; Pichler, MMR 1998, 79, 80; Pelz, ZUM 1998, 530, 532; Roßnagel, NVwZ 1998, 1, 2/3; Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 73; Schuster in: TKG-Kommentar (2. Auflage), § 4 TKG Rn. 4a; Gersdorf in: TKG-Kommentar (3. Auflage), Einleitung C Rn. 20; Manssen in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 3 TKG(1998), Band 1, Rn. 37; Lammich in: Moritz, Rechts-Handbuch zum E-Commerce, B Rn. 243; Richter, Datenschutzrechtliche Aspekte beim Tele- bzw. Homebanking, S. 136; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 76 ff.; Beck-IuKDG-Tettenborn, § 2 TDG Rn. 41; Pelz in: Bräutigam/Leupold, B I. Rn. 45; Pankoke, Von der Presse- zur Providerhaftung, S. 30/31, der aber einen Mittelweg beschreiten möchte, indem er dem jeweiligen Richter überlassen möchte, welche Teile eines Online-Angebots einen einheitlichen Dienst bilden.

[293] Der Begriff der Telekommunikation ist in § 3 Nr. 22 TKG geregelt, wonach Telekommunikation den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen darstellt. Siehe auch OLG Hamburg, CR 2000, 363, 364; Pankoke, Von der Presse- zur Providerhaftung, S. 40; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 71/73; Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 18; Sieber in: Hoeren/Sieber, Teil 19 Rn. 244; Wuermeling/Felixberger, CR 1997, 230, 233/234; Geis, Recht im eCommerce, S. 139; Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2983; Eichhorn, Internet-Recht, S. 35/36/39 (Tabelle); Tettenborn, MMR 1999, 516, 518; Krager in: Königshofen, Das neue Telekommunikationsrecht in der Praxis, S. 117 ff.; Kloepfer, Informationsrecht, § 13 Rn. 19 ff.; siehe auch Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 109; siehe zum Ganzen Imhof, CR 2000, 110, 111. Die Telekommunikation erfasst den Austausch von Informationen durch Transport über gewisse Entfernungen mit Hilfe von technischen Mitteln, während die einzelnen Inhalte der verarbeiteten Nachrichten dagegen nicht dem Telekommunikationsbegriff unterfallen (Schuster in: TKG-Kommentar (2. Auflage), § 1 TKG Rn. 22 sowie Schuster in: TKG-Kommentar (3. Auflage), § 1 TKG Rn. 4; Hoeren, Grundzüge des Internetrechts, S. 259; Engel-Flechsig, RDV 1997, 59, 61).

[294] Vgl. Gersdorf in: TKG-Kommentar (3. Auflage), Einleitung C Rn. 22/23; Schuster in: TKG-Kommentar (2. Auflage), § 4 TKG Rn. 4a; Schuster in: TKG-Kommentar (2. Auflage), § 3 TKG Rn. 21b; Pelz in: Bräutigam/Leupold, B I. Rn. 45. In diesem Sinne auch Pankoke, Von der Presse- zur Providerhaftung, S. 30 ff., der als Anknüpfungspunkt für die Einordnung als Tele-

Gemäß der funktionalen Betrachtungsweise sind die einzelnen Leistungen dieses kombinierten Dienstes als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG, als Teledienst gemäß § 2 Abs. 1 TDG oder als Mediendienst[295] gemäß § 2 Abs. 1 MDStV einzuordnen.[296] Da Mediendienste im Rahmen dieser Arbeit von geringerer Bedeutung sind, bezieht sich diese Abgrenzung im Übrigen ausschließlich auf Telekommunikationsdienste und Teledienste.

---

oder Mediendienst bei einem umfangreichen Online-Angebot auf den Charakter des jeweiligen Inhalts abstellt und innerhalb einer ersten Wertungsstufe die rechtlich relevanten Dienste ermitteln will, um diese in einer zweiten Wertungsstufe unabhängig voneinander als Tele- oder Mediendienst zu qualifizieren. Der Ansicht, die das Anbieten von Diensten im Internet vollständig unter den Begriff der Telekommunikation fassen möchte und deshalb im vollen Umfang das TKG als einschlägig betrachtet (siehe Büchner in: TKG-Kommentar (2. Auflage), § 89 TKG Rn. 11), ist nicht zu folgen. Schmitz (TDDSG und das Recht auf informationelle Selbstbestimmung, S. 72) verweist zu Recht darauf, dass einer solchen Auffassung bereits der Wortlaut von § 3 Nr. 16 TKG a.F. bzw. § 3 Nr. 22 TKG entgegensteht, der den Begriff der Telekommunikation auf den „technischen Vorgang" einschränkt. Die Abgrenzung zwischen Telekommunikationsdiensten und Telediensten wird im Übrigen von § 2 Abs. 4 TDG auch vorausgesetzt (siehe zu letzterem Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 16; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 75; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 70; Engel-Flechsig in: Bartsch/Lutterbeck, Neues Recht für neue Medien, S. 67/69).

[295] Mediendienste i.S.d. § 2 Abs. 1 MDStV sind alle an die Allgemeinheit gerichteten Informations- und Kommunikationsdienste in Text, Ton oder Bild, die unter Benutzung elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters verbreitet werden (siehe zum MDStV Fn. 33). Mediendienste sind redaktionell gestaltet, wobei darunter die planvolle inhaltliche, sprachliche, grafische oder akustische Bearbeitung eines Angebots fällt, mit dem Ziel der Einwirkung auf die öffentliche Meinungsbildung oder Information. Siehe hierzu Gounalakis/Rhode, CR 1998, 487, 489/490; Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 98; Knothe, AfP 1997, 494 ff.; Kuch, ZUM 1997, 225, 228; Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 26; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 75; Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I Rn. 26; Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 81.

[296] Per Definition unterscheiden sich Teledienst und Mediendienst anhand der Merkmale der individuellen Nutzung beim Teledienst einerseits und der Allgemeinadressierung beim Mediendienst andererseits. Kennzeichnend für eine individuelle Nutzung ist, dass die Möglichkeit der Interaktion bzw. der Individualkommunikation im Vordergrund steht (vgl. OLG Hamburg, CR 2000, 363, 364; v. Heyl, ZUM 1998, 115, 118; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 80 ff.; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 75; Spindler in: Roßnagel, Recht der Multimedia-Dienste, § 2 TDG Rn. 18; Scholz in: Roßnagel, Datenschutz beim Online-Einkauf, S. 42/43; Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I Rn. 5, 39; Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 74). Im Unterschied dazu ist bei der Massenkommunikation ein Angebot an die Allgemeinheit gerichtet, so dass eine Kommunikation zwischen Sender und Empfänger nur auf Umwegen möglich ist. Siehe zu letzterem: v. Heyl, ZUM 1998, 115, 118; vgl. auch Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 98; Pankoke, Von der Presse- zur Providerhaftung, S. 40; Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 79; vgl. auch Spindler/Volkmann, K&R 2002, 398, 399; Zimmermann, NJW 1999, 3145, 3146; Scholz in: Roßnagel, Datenschutz beim Online-Einkauf, S. 43, der anmerkt, dass im Rahmen des TDG der Nutzer auf das Angebot „unmittelbar", das heißt ohne Medienbruch etwa aus dem Web-Browser heraus, reagieren kann. Siehe zum Medienbruch auch den „Bericht der Bundesregierung über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG)", Bundestag-Drucksache 14/1191, S. 7 (nachfolgend: Bundestag-Drucksache 14/1191), wo es heißt, dass in wichtigen Angebots- und Nutzungsbereichen eine eindeutige Zuordnung als Tele- oder Mediendienst möglich sei und beispielhaft unter anderem der „Fernseheinkauf mit Medienbruch (per Telefon)" genannt wird.

Nach § 3 Nr. 24 TKG sind Telekommunikationsdienste

- gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich der Übertragungsdienste in Rundfunknetzen,

wohingegen Teledienste gemäß § 2 Abs. 1 TDG

- alle elektronischen Informations- und Kommunikationsdienste darstellen, die für eine individuelle Nutzung von kombinierbaren Daten, wie Zeichen, Bilder oder Töne bestimmt sind, und denen eine Übermittlung mittels Telekommunikation zugrunde liegt („Individualkommunikation").[297]

Diese Trennung zwischen Inhalt und Übertragung entspricht im Übrigen den Vorgaben der EU-Richtlinie 2002/58/EG.[298]

2. Neues Begriffsverständnis

Diese auf der funktionalen Betrachtungsweise basierende Unterteilung in ein Zwei-Personen-Verhältnis sowie in eine Transport- und Inhaltsebene ist für diese Arbeit aus den folgenden Gründen nicht zielführend.

[297] Siehe Schaar, Datenschutz im Internet, Rn. 308.

[298] Die Richtlinie trennt ebenfalls zwischen Nachrichtenübertragungen, also der rein technischen Seite, sowie den Vorgängen, die über diese rein technische Seite hinausgehen. Letzteres wird in Artikel 2 g) der Richtlinie als „Dienst mit Zusatznutzen" definiert. Gemäß dieser Begriffsbestimmung gilt damit als eigentlicher Kommunikationsdienst die reine Nachrichtenübermittlung, wohingegen gemäß Erwägungsgrund 18 der EU-Richtlinie 2002/58/EG unter den Begriff „Dienst mit Zusatznutzen" diejenigen Dienste fallen, die über die Nachrichtenübermittlung hinausgehen. Erwägungsgrund 18 der EU-Richtlinie 2002/58/EG erwähnt hier unter anderem beispielhaft Navigationshilfen, touristische Informationen und Wettervorhersage. Dies entspricht dem geltenden deutschen Recht insoweit, als dies den Definitionen im Sinne des § 2 Abs. 1 TDG und Telediensten gleich kommt (siehe auch Engel-Flechsig, DuD 1997, 8, 12, der als Angebot zur Nutzung des Internet ebenso Navigationshilfen beispielhaft nennt sowie bei den Angeboten zur Information und Kommunikation sowohl auf den Gesetzestext und Angebote wie Verkehrs-, Wetter-; Umwelt- und Börsendienste verweist als auch Homepages beispielhaft nennt.). Es soll jedoch an späterer Stelle näher untersucht werden (siehe S. 102 ff.), ob der „Dienst mit Zusatznutzen" im Sinne der EU-Richtlinie 2002/58/EG mit dem geltenden Begriff des Teledienstes übereinstimmt. Siehe außerdem Eckhardt, CR 2003, 805, 805, der darauf hinweist, dass hierdurch die Möglichkeit nahe gelegt wurde, das Datenschutzrecht für elektronische Kommunikation unter Aufgabe der Eigenständigkeit des Teledienstedatenschutzgesetzes (TDDSG) zu vereinheitlichen. Dies sei jedoch im Hinblick auf die unterschiedlichen Regelungsansätze und die Kompetenzverteilung zwischen Bund und Ländern sowie den zeitlichen Druck der Umsetzung unterlassen worden.

a. Berücksichtigung des Mehrpersonenverhältnisses

Das gebräuchliche Begriffsverständnis des Online-Dienstes bezeichnet entweder einen großen, kommerziellen Anbieter[299]oder das (kombinierte) Dienstleistungsangebot eines (einzigen) Anbieters.[300]
Dies indiziert eine rechtliche Prüfung ausschließlich in einem Zwei-Personenverhältnis, zwischen einem (großen, kommerziellen) Anbieter und einem Nutzer, ohne auf die Verflechtung der unterschiedlichen beteiligten Interessen und Personen dieses Komplettpakets zu achten.

Die herkömmliche Betrachtung verschleiert, dass der Nutzer eines Dienstes gleichzeitig Anbieter des Dienstes für andere sein kann. Ihm können unter Umständen eigene datenschutzrechtliche Pflichten gegenüber weiteren Beteiligten obliegen, deren Sicherstellung bereits bei der inhaltlichen Ausgestaltung des Vertragsverhältnisses mit seinem Anbieter beachtet werden sollten.
Soll -wie in dieser Arbeit- eine Gesamtaussage zu den datenschutzrechtlichen Erfordernissen eines Dienstes und dessen datenverarbeitenden Systemen getroffen werden, so muss der Dienst in seiner Gesamtheit betrachtet werden.

---

[299] Siehe oben Fn. 283/284. Ebenso Lammich in: Moritz, Rechts-Handbuch zum E-Commerce, B Rn. 245, der T-Online als Gesamtdienst bzw. Komplettpaket bezeichnet.
[300] OLG Hamburg, CR 2000, 363, 363; Beck-IuKDG-Engel-Flechsig, Glossar S. 830; Koch, Internet-Recht, S. 4; Eichhorn, Internet-Recht, S. 42; Schaar, Datenschutz im Internet, Rn. 304; Hoeren, MMR 1999, 192, 195; Tettenborn, MMR 1999, 516, 518; Schneider, MMR 1999, 571, 575; Ory, AfP 1996, 105, 105. Siehe außerdem Ritz, Inhalteverantwortlichkeit von Online-Diensten, S. 67, die hier entgegen ihrer vorherigen Definition von Online-Diensten als Anbieter, wie etwa AOL, CompuServe, T-Online (S. 20), Online-Dienste als Tele- bzw. Datendienste bezeichnet; Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 72 (wo nicht ganz klar wird, ob nun der Anbieter selbst gemeint ist oder dessen inhaltlichen Angebote, aber die gemachten Ausführungen auf beides zutreffen können). Spindler, MMR-Beilage 2000, 4, 5 verweist auf den ursprünglichen Richtlinienvorschlag zu „bestimmten rechtlichen Aspekten des elektronischen Geschäftsverkehrs im Binnenmarkt“ verweist (KOM (1998) 585 endg.; ABl. EG Nr. C 30 vom 05.02.1999, S. 4 ff.). Ruppmann, Der konzerninterne Austausch personenbezogener Daten, S. 40 verwendet den Begriff „Online-Dienste“ im Zusammenhang mit dem konzerninternen Angebot des Autoherstellers Volvo an seine Händler; siehe auch Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 103, wo auf die Angebote des ZDF verwiesen und dabei ebenfalls der Online-Dienst im Sinne eines inhaltlichen Angebots verstanden wird. Siehe in diesem Sinne ebenso Hoeren, Grundzüge des Internetrechts, S. 261, der ausführt, dass derselbe Diensteanbieter verschiedene Online-Dienste anbieten kann. Vgl. außerdem Schulz, ZUM 1996, 487, 487, der den Begriff des Online-Dienstes als Dienstleistung versteht, bei denen ein Nutzer auf Abruf Informationen eines Anbieters über ein Datennetz erhalten kann, aber auf der anderen Seite darauf verweist (Schulz, ZUM 1996, 487, 494), dass es der Gesetzgeber bei Online-Diensten ebenso mit Plattformen (wie T-Online, Compuserve und AOL) zu tun hat.

Daher sollte der Begriff „Online-Dienst" losgelöst von einem festen Anbieter und Nutzer verstanden werden, so wie es der EU-Richtlinie 98/34/EG entspricht.[301] Für die Herleitung eines neuen Begriffsverständnisses ist insbesondere Artikel 2 b) und Artikel 2 d) der Richtlinie 98/34/EG heranzuziehen. Daraus ergibt sich, dass ein Diensteanbieter auch gleichzeitig Nutzer ist, da unter diese Definition derjenige fällt, der Informationen für andere zugänglich macht und sich dabei eines Dienstes der Informationsgesellschaft bedient.[302]

Unter Berücksichtigung der Legaldefinition des Begriffs „Dienst" in Artikel 1 Nr. 2 der Richtlinie 98/34/EG, wonach ein Dienst eine Dienstleistung[303] der

---

[301] Auf de Richtlinie 98/34/EG wird in Artikel 2 a) der Richtlinie 98/48/EG verwiesen. Siehe Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20.07.1998 zur Änderung der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften, ABl. Nr. L 217 vom 05.08.1998, S. 18 (nachfolgend: Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG).

[302] Siehe Glatt, Vertragsschluss im Internet, S. 75, der zum einen darauf verweist, dass der Begriff des Diensteanbieters, wie er von der Richtlinie gemäß Artikel 2 b) verwendet wird, nicht mit dem Service Provider im technischen und umgangssprachlichen Sinne gleichgesetzt werden darf, da Diensteanbieter im Verhältnis zum Nutzer vielmehr auch derjenige ist, wer unter Einschaltung eines Internet Providers eigene Inhalte zur Verfügung stellt. Zum anderen sei ein solcher Anbieter aber gleichzeitig auch Nutzer, da unter die Definition des Artikel 2 d) auch derjenige fällt, der Informationen für andere zugänglich macht und sich dabei eines Dienstes der Informationsgesellschaft bedient. Damit sei Nutzer nicht nur, wer als Kunde beispielsweise ein WWW-Angebot in Anspruch nimmt, sondern auch der Anbieter selbst im Verhältnis zu seinem Provider, der ihm den Internet-Auftritt ermöglicht.

[303] „Dienstleistung" bezeichnet gemäß Artikel 49, 50 EG-Vertrag (Vertrag zur Gründung der Europäischen Gemeinschaft in der Fassung vom 02.10.1997, geändert durch den Vertrag von Nizza vom 26.02.2001 (ABl. Nr. C 80 vom 10.03.2001, S. 1; siehe hierzu ebenso Erwägungsgrund 19 der EU-Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG, der auf die Regelungen des EG-Vertrags verweist) insbesondere die gewerbliche, kaufmännische, handwerkliche und freiberufliche Tätigkeit, wobei aber weder verlangt wird, dass ein Provider, um als Anbieter einer Dienstleistung qualifiziert zu werden, ein ganzes Leistungspaket anbieten muss, noch dass andererseits ein und derselbe Provider nicht genauso gut eine Vielzahl verschiedener Dienste anbieten könnte (Vgl. Erwägungsgrund 18 des Vorschlags der Kommission der europäischen Gemeinschaften für eine Richtlinie des europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt vom 18.11.1998 KOM (1998) 586 endg. (nachfolgend: Vorschlag der Kommission), sowie Glatt, Vertragsschluss im Internet, S. 71. Siehe außerdem Pankoke, Von der Presse- zur Providerhaftung, S. 30, der darauf verweist, dass ein umfangreiches Online-Angebot aus mehreren „Diensten" bestehen kann, und dass in diesem Falle jeder von ihnen gesondert als Tele- bzw. Mediendienst einzustufen ist. Siehe außerdem auch Beck-IuKDG-Tettenborn, § 2 TDG Rn. 39, der sowohl die Erbringung von Telekommunikation, Rundfunk als auch Telediensten unter den Dienstleistungsbegriff nach Artikel 59, 60 EGWV (nunmehr Artikel 49, 50 EG-Vertrag) subsumiert. Vgl. ebenso Dörr, NJW 1995, 2263, 2265 zum Bereich des Rundfunks.
Ebenso wenig ist außerdem erforderlich, dass die fragliche Dienstleistung nur gegen Entgelt angeboten wird (vgl. hierzu auch Vorschlag Kommission, S. 17 und Artikel 1 Nr. 2 der Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG, in welchem definiert ist, dass die Dienstleistung in der Regel, also nicht notwendigerweise, gegen Entgelt erbracht wird). Vgl. außerdem die Anmerkung von Hoeren, MMR 1999, 192, 193, dass der Begriff der „Dienstleistung" hier nicht im Sinne des deutschen Dienstvertragsrechts missverstanden werden sollte.

Informationsgesellschaft ist,[304] d.h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, empfiehlt es sich folglich, den Begriff des Online-Dienstes in seine Wortbestandteile zu zerlegen.

Dementsprechend wird vorgeschlagen, einen Online-Dienst wie folgt zu definieren**:**

*Bei einem Online-Dienst handelt es sich insgesamt um eine wirtschaftliche Tätigkeit[305](**=Dienstleistung**), die im Internet erbracht wird und/oder in der Verbindung zum Internet besteht,[306] also um eine ausschließlich elektronisch*

---

[304] Der Begriff „Dienst der Informationsgesellschaft" ist im Übrigen insoweit „neutral", dass er keine Vorfestlegung bezüglich Telekommunikationsdiensten, Telediensten oder Mediendiensten beinhaltet. Dies gilt auch bezüglich des ursprünglichen Richtlinienvorschlags der E-Commerce-Richtlinie (Fn. 27), der durch seine abstrakt gehaltene Begriffsdefinition auch über Telefon oder Fax abgewickelte Abrufdienste erfasste, siehe hierzu Spindler, MMR-Beilage 7/2000, 4, 5. Auch Erwägungsgrund 10 der Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG geht davon aus, dass von dem Begriff „Dienst der Informationsgesellschaft" grundsätzlich auch Telekommunikationsdienste erfasst sind, wobei die Unterrichtungspflicht nach der EU-Richtlinie aber nur dann in Betracht kommen soll, sofern das geltende Gemeinschaftsrecht nicht bereits Regelungen vorsieht. In Anhang V sind allerdings ausdrücklich Telefon- und Faxdienste ausgenommen.

[305] Vgl. zur wirtschaftlichen Tätigkeit den Vorschlag der Kommission, S. 16/17 sowie Fn. 303, wo darauf hingewiesen wurde, dass es sich insgesamt um ein Leistungspaket oder um eine Einzelleistung handeln kann. Siehe auch Hoeren, MMR 1999, 192, 193, der auf die Abgrenzungsschwierigkeiten bei einer wirtschaftlichen Tätigkeit verweist. Hier ist aber festzustellen, dass wirtschaftlich nicht zwangsläufig mit kommerziell bzw. gewinnorientiert gleichzusetzen ist (siehe hierzu auch Hoeren, MMR 1999, 192, 193, der auf den nicht kommerziellen Universitätsbetrieb verweist). In diesem Sinne ist nunmehr auch das TKG umgesetzt worden (und zuvor bereits die TDSV geändert worden, da der Begriff der Gewerblichkeit als Voraussetzung eines Telekommunikationsdienstes gestrichen worden ist (vgl. hierzu ebenso Fn. 31 und S. 117 ff. sowie Zimmer, CR 2003, 893, 896, die darauf verweist, dass der Gesetzgeber bewusst auf die Gewerblichkeit verzichtet hat)), und darüber hinaus § 3 Nr. 24 TKG nicht voraussetzt, dass bei einem Telekommunikationsdienst „geschäftsmäßiges" Handeln vorliegen muss (siehe ebenso Hoeren aaO, der darauf verweist, dass klar gestellt werden sollte, dass die Mitgliedstaaten bei der Umsetzung der E-Commerce-Richtlinie (siehe zur E-Commerce-Richtlinie Fn. 27) den Anwendungsbereich auch auf nicht-kommerzielle Provider ausdehnen können).

[306] So geht außerdem die E-Commerce-Richtlinie (Fn. 27) in Erwägungsgrund 18 davon aus, dass „Dienste der Informationsgesellschaft" ebenso Dienste sind, die Zugang zu einem Kommunikationsnetz anbieten; siehe in diesem Sinne auch Spindler, MMR-Beilage 7/2000, 4, 5 mit dem Hinweis, dass auch Access-Provider erfasst werden. Dies ergibt sich ebenso aus Artikel 1 Abs. 5 b) der EU-Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG, der regelt, dass diese Richtlinie keine Anwendung findet auf Fragen betreffend die Dienste der Informationsgesellschaft, die von den Richtlinien 95/46/EG (siehe Richtlinie des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABL. EG Nr. L 281 vom 23.11.1995, S. 31) und 97/66/EG erfasst werden. Siehe außerdem Cichon, Internetverträge, Rn. 1, die im Hinblick auf Internetverträge ausführt, dass diese entweder das Internet selbst im weiteren Sinne zum Gegenstand haben oder aber im Internet geschlossen werden. A.A. aber Mehrings, CR 1998, S. 613 ff., der Internetverträge in einem engeren Begriffverständnis auslegt und darunter ausschließlich Verträge versteht, die im Internet geschlossen werden. Vgl. hierzu

(=online)[307] *erbrachte Dienstleistung.*[308]

Die gängige Auslegung des Begriffs „Online-Dienstes“ ist nicht nur überholt,[309] sondern aufgrund der oben angesprochen uneinheitlichen Begriffsverwendung als Synonym für große, kommerzielle Anbieter von Online-Dienstleistungen unzweckmäßig.

b. Berücksichtigung sämtlicher Leistungen

Eine Trennung eines kombinierten Online-Dienstes (ausschließlich) in eine Transport- und Inhaltsebene im Sinne einer funktionalen Betrachtungsweise[310] berücksichtigt außerdem nicht, dass innerhalb eines kombinierten Dienstes auch mehrere Transportebenen in Betracht kommen können. Dies kann sowohl bei der Bereitstellung der Online-Dienstleistung durch einen einzigen Anbieter gelten. Die Aufteilung des Dienstes in mehrere Transportebenen kann jedoch

---

auch Glatt, Vertragsschluss im Internet, S. 71, 73, der auf das Verständnis der Europäischen Kommission Bezug nimmt, wonach der elektronische Geschäftsverkehr aus Diensten der Informationsgesellschaft und diese wiederum aus einer Vielzahl unterschiedlicher Online-Dienste besteht. Als Online-Dienste werden hierbei beispielhaft der Warenverkauf oder Dienstleistungen oder freie Bereitstellung von Informationsangeboten, die über kommerzielle Kommunikationen finanziert werden, genannt (Vorschlag der Kommission, S. 7). Er verweist ebenfalls darauf, dass in der Begründung zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt“ (Vorschlag der Kommission, S. 17) Dienste, die den Zugang zum World Wide Web vermitteln, als Beispiel für die Dienste der Informationsgesellschaft aufgezählt sind.

[307] Für den Begriff „online“ ist eine physische Datenverbindung ausreichend, über die eine Datenübertragung erfolgt, so dass davon bereits eine Datenübertragung von einem Rechner zu einem Drucker erfasst ist (siehe zu „online“ Voss, Das große PC Lexikon 2007, S. 587; vgl. auch Auernhammer, BDSG, § 3 BDSG Rn. 38). In diesem Sinne wird der Begriff „Online“ auch folgerichtig als ein Betriebszustand beschrieben, in dem ein Datenendgerät mit einem anderen Computer verbunden ist (Hobert, Datenschutz und Datensicherheit im Internet, S. 229; vgl. auch Wanckel, Persönlichkeitsschutz in der Informationsgesellschaft, S. 63, der den Begriff „Echtzeitverbindung“ verwendet und damit die Möglichkeit des unmittelbaren Datendialogs mit kurzen Antwortzeiten vorsieht. Siehe m.w.N. auch Ehmann in: Simitis, BDSG-Kommentar, § 10 BDSG Rn. 36, der anmerkt, dass der Begriff „online“ schillernd ist).

[308] Siehe Fn. 303, wo festgestellt worden ist, dass im Sinne der Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG ein Online-Dienst folgerichtig sowohl aus einem einzigen Telekommunikations-, Tele- oder Mediendienst als auch aus einem Gesamtangebot bzw. aus einer kombinierten Dienstleistung bestehen kann (und damit nicht notwendigerweise ein gesamtes Leistungsbündel umfasst).

[309] Insbesondere entspricht auch die Definition, dass Online-Dienste eigene geschlossene und zentral strukturierte Netze betreiben, die nur ihren registrierten Nutzern offen stehen nicht mehr den heutigen Leistungsformen (vgl. hierzu Fn. 284). Besucht ein Nutzer die Homepages von T-Online oder AOL, so findet er dort ein reichhaltiges Angebot an Online-Shopping-, Reise-, Chat-Angeboten, etc., so dass die Begrenzung auf einen registrierten Nutzerkreis entfällt. Diese Definition passte damit zwar zu den Anfängen des Internetzeitalters, ist aber mittlerweile überholt.

[310] Siehe zur funktionalen Betrachtungsweise S. 66.

gleichermaßen erforderlich sein, wenn an der Bereitstellung der Online-Dienstleistung mehrere Anbieter beteiligt sind.

So wird in dieser Arbeit das Komplettpaket VPN in jedwedem Personenverhältnis in seine einzelnen Dienstleistungen aufgespalten. Innerhalb dieser Personenverhältnisse werden diese „Einzel-Dienstleistungen“ betrachtet und rechtlich als Telekommunikationsdienstleistung oder als Teledienst eingeordnet. Das Hauptaugenmerk liegt jedoch nicht in der Trennung zwischen Transportebene (TKG) und Inhaltsebene (TDG/TDDSG), sondern in der Betrachtung der jeweiligen Dienstleistung. Dies führt dazu, dass mehrere Telekommunikationsdienstleistungen und damit mehrere Transportebenen innerhalb des Komplettpakets nebeneinander stehen können, deren datenschutzrechtliche Relevanz geprüft wird.

c. Konsequenz: Dienstorientierte Betrachtung im Mehrpersonenverhältnis

Für diese Arbeit bedeutet dieses neue Begriffsverständnis, dass unter dem Oberbegriff „Online-Dienst und Datenschutz“ jedwedes Personenverhältnis in einem (Internet-)VPN rechtlich untersucht werden kann, einschließlich des Datenschutzes eines Betroffenen, der den Dienst nicht unmittelbar selbst in Anspruch nimmt.
Außerdem wird der Begriff des „Online-Dienstes“ nicht für wenige, große kommerzielle Anbieter monopolisiert. Eine solche Monopolisierung wäre zudem falsch, da durch die Liberalisierung auf dem Telekommunikationsmarkt die Anbietervielfalt heutzutage zu groß ist, ohne dass eine gewisse Eigentümlichkeit (Proprietät) der Angebote bei den unterschiedlichen Diensteanbietern festgestellt werden könnte

Die Aufspaltung des VPN in seine einzelnen Bestandteile führt dazu, dass die funktionale Betrachtungsweise erweitert wird, so dass die Abgrenzung der Dienstleistungen innerhalb eines kombinierten Online-Dienstes nicht entweder (nur) transportbezogen oder (nur) inhaltsbezogen erfolgt, sondern der hauptsächliche Bezugspunkt darin liegt, die „Einzel“-Leistungen eines solchen Komplettpakets in jedem einzelnen Personenverhältnis rechtlich zu bewerten.

Damit wird die Einteilung in mehrere Transport- und Personenebenen zugelassen.
Daher ist insgesamt der Begriff der dienstorientierten anstatt der funktionalen Betrachtungsweise passender: Die Aufspaltung des kombinierten Dienstes wird anhand seiner einzelnen Leistungsbestandteile und nicht an einer Transport- oder Inhaltsebene orientiert vorgenommen.
Zur Klarstellung soll aber darauf verwiesen werden, dass die Unterscheidung zwischen Transport- und Inhaltsebene für die Anwendbarkeit des TDDSG oder TKG im Rahmen *einer Einzelleistung* eines kombinierten Online-Dienstes (nach wie vor) erforderlich ist.

Diese Begriffsdefinition der dienstorientierten Betrachtungsweise ist zudem für andere komplexe Dienstleistungen bedeutsam, beispielsweise Dienstleistungen wie Application Service Providing (ASP) und Online-Backup-Lösungen, die ebenso ein ganzes Leistungsbündel beinhalten.[311] Die eigentlich charakteristische Leistung des Application Service Providing besteht darin, einem Nutzer per Fernzugriff über das Internet die Benutzung von Anwendungssoftware zu erlauben.[312] Bei Online Backup Lösungen handelt es

[311] Siehe Bettinger/Scheffelt, CR 2001, 729, 730
[312] v.Westerholt/Berger, CR 2002, 81, 81; Intveen/Lohmann, ITRB 2002, 210, 210; Koch, Internet-Recht, S. 10/11; Peter, CR 2005, S. 404 ff. Die IT-Systeme befinden sich physisch beim Provider. Der Provider bedient sich öffentlicher Kommunikationsnetze, vor allem des Internets, um den Kunden den Zugriff auf den beim Provider installierten Server samt Software zu ermöglichen (Grützmacher, ITRB 2001, 59, 59; vgl. auch Peter, CR 2005, S. 404, 405). Hierbei wird auf einen zentralen Server des Providers zugegriffen, und zwar ohne dass sich der Nutzer die entsprechende Software auf seinen eigenen Rechner installiert (Röhrborn/Sinhart, CR 2001, 69, 69; vgl. zu ASP ebenso Gottschalk in: Kaminski/Henßler/Kolaschnik/Papathoma-Baetge, Rechtshandbuch E-Business, S. 722 ff.). ASP wird stets im Zusammenhang mit Unternehmen, insbesondere Kostenreduzierung der Unternehmen genannt, so etwa, dass ASP im allgemeinen Trend der Wirtschaft zu „schlanken" Unternehmen steht, die sich auf ihre Kerngeschäftsfelder konzentrieren, und zum Ziel hat, die immer komplexer werdenden Softwareanwendungen aus dem jeweiligen Unternehmen heraus zu verlagern und einem speziellen Dienstleister zu übertragen (vgl. auch Czychowski/Bröcker, MMR 2002, 81, 81). Beliebter Einsatzort für ASP ist vor allem auch der Bereich des Customer Relationship Management. Gesammelte Informationen über Kunden werden aus verschiedenen Geschäftsbereichen zusammengefügt, einheitlich verwaltet und analysiert, und diese Datenbank mittels ASP bereitgestellt. Zum Application Service Providing als Outsourcing-Modell siehe Gennen, ITRB 2002, 291, 291; Czychowski/Bröcker, MMR 2002, 81, 81; Bettinger/Scheffelt, CR 2001, 729, 729 (Bettinger/Scheffelt, CR 2001, 729, 731 und Dick, ASP-Magazin 6/2000, 40, 42 verweisen ebenso darauf, dass es sich bei ASP-Verträgen um komplexe Langzeitverträge handelt, in der Regel zwei bis fünf Jahre). Siehe zu ASP außerdem Martens/Schwarz-Gondek in: Bräutigam/Leupold, Glossar S. 1067. Siehe außerdem zum ASP-Geschäftsmodell Bettinger/Scheffelt in: Spindler, Vertragsrecht der Internet Provider, Teil XI Rn. 1 ff. sowie zum Charakter eines komplexen Langzeitvertrages Rn. 16.

sich um eine neue Form des Host-Service, bei denen der Nutzer seine Daten auf dem ihm vom Provider zur Verfügung gestellten Speicherplatz sichert. [313] Application Service Providing und Backup-Lösungen können ebenso mit einem VPN verknüpft werden,[314] worauf an späterer Stelle in dieser Arbeit noch näher eingegangen wird.[315]

3. Abgrenzung zu Internet-Diensten

Im Sinne einer klaren Begriffsdefinition und als Grundlage für eine rechtliche Prüfung im dritten und vierten Abschnitt dieser Arbeit muss ein „Online-Dienst" zudem von einem „Internet-Dienst" abgegrenzt werden. Die nähere Erläuterung der Internet-Dienste empfiehlt sich in diesem Abschnitt „Materielle Grundlagen" im unmittelbaren Anschluss an die Definition der Online-Dienste, um deutlich

---

[313] Vgl. die Produkte unter http://www.interscholz.net/produkte/business/18 sowie http://www.pop-i.de/de/security/security_backup.php (Websites vom 30.09.2006). . Siehe außerdem Schaar, Datenschutz im Internet, Rn. 25, der auf die Neuheit des Dienstes. Bei Online-Backup-Lösungen ist es von besonderer Bedeutung, dass die Daten verschlüsselt übertragen. Die Online-Backup-Lösungen bieten die Möglichkeit, die Datensicherung von Unternehmensdaten komplett auszulagern und auf fremden Servern zu speichern (Datenhosting), so dass auf die Anschaffung eigener, umfangreicher Hardwarekapazitäten verzichtet werden kann (siehe auch Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil V Rn. 4; Schuppert, CR 2000, 227, 230 zum Datenhosting sowie zur damit verbundenen Bereitstellung eines ftp-Zugangs). So wurde das Hosten von Daten regelmäßig auf das Website-Hosting eingegrenzt, was unter Umständen auch daran liegen mag, dass die Allgemeinen Haftpflichtbedingungen (AHB) Schäden, die aufgrund des Datenverlustes als reine Vermögensschäden entstehen nicht abdecken (vgl. Frankfurter Allgemeine Zeitung vom 19. Januar 2002, S. 19), so dass viele Unternehmen noch aufgrund der Haftungsrisiken vor einem solchen Angebot zurückschrecken. Zum Begriff des Hosting siehe: Geis, Recht im eCommerce, S.109; Härting, CR 2001, 37, 37/39; Pelz in: Bräutigam/Leupold, B I. Rn. 44; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 12; Röhrborn/Sinhart, CR 2001, 69, 73; Cichon, Internetverträge, Rn. 160; Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil V Rn. 15 ff.; Komarnicki in: Hoeren/Sieber, Teil 12.2 Rn. 4; Pankoke, Von der Presse- zur Providerhaftung, S. 170. Hierbei ist anzumerken, dass der Begriff des Hosting regelmäßig als Website-Hosting verstanden wird, also dahingehend, dass der Provider die Website seines Kunden Dritten im Internet zugänglich macht (vgl. etwa Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 42; Schuppert, CR 2000, 227, 228; Cichon, Internetverträge,Rn. 160; Komarnicki in: Hoeren/Sieber, Teil 12 Rn. 4, teia (Hrsg.), Recht im Internet, S. 633 „Web-Hosting", „Webspace"; Schneider, Verträge über Internet-Access, S. 98). Die Voraussetzungen von Website-Hosting und Hosting sind jedoch dieselben, da in beiden Fällen dem Nutzer Speicherplatz zur Speicherung seiner Daten überlassen wird, wobei der einzige Unterschied darin bestehen soll, dass bei Datenhosting keine Anbindung an das Internet, sondern die Abrufbarkeit durch den Nutzer geschuldet ist (Röhrborn/Sinhart, CR 2001, 69, 73 Fn. 46). Dieser Meinung kann jedoch lediglich gefolgt werden, soweit es um die Feststellung geht, dass Datenhosting und Website-Hosting die gleichen Voraussetzungen haben. Denn selbstverständlich schuldet auch der Datenhost-Provider die Anbindung des Servers an das WWW, da ansonsten für den Kunden kein Datenabruf bzw. Datentransfer möglich wäre.

[314] Vgl. hierzu beispielsweise Lipp, VPN, S. 399.

[315] Siehe zum Application Service Providing S. 310, 413, 428, 439. Siehe zum Online Backup S. 312, 341, 346, 348.

aufzuzeigen zu können, dass Internet-Dienste eine andere inhaltliche Bedeutung als Online-Dienste haben. Die Begriffe sind nicht synonym zu verwenden, auch wenn im allgemeinen Sprachgebrauch zwischen „Internet-Dienst“ und „Online-Dienst“ kein Unterschied gemacht wird.
Unter „Internet-Diensten“ werden im Wesentlichen das World Wide Web (WWW), Newsgroups, Chatrooms, file transfer protocol (ftp), telnet und der E-Mail-Dienst verstanden.[316] Hierbei handelt es sich um technische Möglichkeiten bzw. Funktionalitäten des Internet, die die Grundlagen von Kommunikationsvorgängen im Internet bieten.[317]
Auf TCP/IP setzen Internet-Dienste im Internet auf,[318] benötigen also TCP/IP als Grundvoraussetzung für die Übertragung.
So nutzt der ftp-Service das „file transfer protocol“ (ftp),[319] der E-Mail-Dienst[320] das „post office protocol“ (POP3) und das „simple mail transfer protocol“ (SMTP) zum Empfang und Versendung individueller Nachrichten,[321] Usenet das „network news transfer protocol“ (NNTP) zur Verbreitung von Newsgroup-Nachrichten, und der Internet Relay Chat (IRC) das gleichnamige Protokoll[322]

[316] Schaar, Datenschutz im Internet, Rn. 12 ff.; Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 83 ff; Hobert, Datenschutz und Datensicherheit im Internet, S. 37 ff.; Eichhorn, Internet-Recht, S. 21 ff.; teia (Hrsg.), Recht im Internet, S. 31 ff.; Kröger/Kuner, Internet für Juristen, S. 10 ff.; Schneider, Verträge über Internet-Access, S. 96/97; Wildemann, Vertragsschluss im Netz, S. 4; Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 4 ff; Dilger, Verbraucherschutz bei Vertragsabschlüssen im Internet, S. 13 ff.; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 9/10; Glatt, Vertragsschluss im Internet, S. 17 ff; Ritz, Inhalteverantwortlichkeit von Online-Diensten, S. 21 ff.; Kröger/Göers/Hanken, Internet für Juristen, S. 13 ff.; Summa in: Holznagel/Nelles/Sokol, TKÜV, S. 27 ff.; Blümel/Soldo, Internet-Praxis für Juristen, S. 31 ff.; siehe auch Wanckel, Persönlichkeitsschutz in der Informationsgesellschaft, S. 63/70, der ebenfalls zwischen Online-Diensten und Internet-Diensten trennt; siehe aber auch Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 70 ff., der die Begriffe „Internet“ und „Online“ im Zusammenhang mit einem Dienst synonym verwendet.
[317] Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 83 ff. Siehe zu den Internet-Diensten www, ftp, gopher und telnet: Holznagel in: Hoeren/Sieber, Teil 3.2 (bis zur 5. Ergänzungslieferung) Rn. 54 und nunmehr Holznagel/Kibele in: Hoeren/Sieber, Teil 5 Rn. 68. Siehe zu den Internet-Diensten außerdem Sieber in: Hoeren/Sieber, Teil 1 Rn. 79 ff.
[318] Siehe etwa Hobert, Datenschutz und Datensicherheit im Internet, S. 37; teia (Hrsg.), Recht im Internet, S. 32; Schneider, MMR 1999, 571, 571.
[319] Siehe zu ftp S. 23.
[320] Der E-Mail Dienst nimmt demgemäß eine „Zwitterstellung“ ein und stellt sowohl einen Online-Dienst als auch einen Internet-Dienst dar. Vgl. hierzu und zum E-Mail-Dienst auch Sieber in: Hoeren/Sieber, Teil 1 Rn. 79/114; Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 26, S. 83; Schaar, Datenschutz im Internet, Rn. 12; Hobert, Datenschutz und Datensicherheit im Internet, S. 38; Eichhorn, Internet-Recht, S. 21, 25; teia (Hrsg.), Recht im Internet, S. 34.
[321] Siehe zu SMTP sowie dem E-Mail-Dienst im Besonderen S. 23/63.
[322] Siehe zu „IRC“ Voss, Das große PC & Internet Lexikon 2007, S.473).

zur Echtzeitkommunikation[323] mit anderen Internetnutzern.[324] Im WWW wird die Übertragung von Dateien, die in der Programmiersprache „hyper text markup language“ (html) verfasst sind, durch das „hyper text transfer protocol“ (http) bewerkstelligt.[325] Auch Telnet, wobei der entsprechende Telnet-„Service“ ebenfalls als Internet-Dienst qualifiziert wird,[326] ist ein Netzwerk-Terminal-Protokoll.[327]

Die Internet-Dienste sind gleichbedeutend mit Kommunikationsvorgängen zu sehen.[328] Online-Dienste (sowohl im Sinne des herkömmlichen Begriffsverständnisses als auch im Sinne der hier gemachten Definition) bzw. die einzelnen Angebote innerhalb eines Online-Dienstes betreffen hingegen vorrangig die wirtschaftlichen Tätigkeiten, die sich über das Netz abwickeln lassen.[329]

Dies zeigt aber, dass es ohne diese technischen Grundlagen der Internet-Dienste keine Online-Dienste gäbe. Denn so haben Internet-Dienste gemein, dass sie die Voraussetzung für die Verständigung zwischen den Nutzern bzw. den Rechnern im Internet bilden, indem sie gleiche Protokolle nutzen.[330] Aufgrund dieser Protokolle können Internet-Dienste bestimmte Konventionen zur Verarbeitung und Darstellung der Daten beachten, so dass bei Verwendung einer entsprechenden Software eine weltweite Datenübermittlung möglich ist.[331]

So stellt die Möglichkeit, Daten mittels ftp zu übertragen, einen Dienst dar, den das Internet aufgrund seiner technischen Struktur zur Verfügung stellt. Das

[323] Siehe zur Definition der Echtzeitdienste Dilger, Verbraucherschutz bei Vertragsabschlüssen im Internet, S. 15.

[324] Vgl. Cichon, Internetverträge,Rn. 28; teia (Hrsg.), Recht im Internet, S. 32 ff.; zu dem Protokoll NNTP siehe auch Sieber in: Hoeren/Sieber, Teil 1 Rn. 146 sowie Blümel/Soldo, Internet-Praxis für Juristen, S. 25.

[325] Siehe hierzu bereits S. 23.

[326] Siehe etwa Hobert, Datenschutz und Datensicherheit im Internet, S. 45; Eichhorn, Internet-Recht, S. 27; Kröger/Kuner, Internet für Juristen, S. 20; Schneider, MMR 1999, 571, 572; siehe zur Begriffserläuterung von „Telnet“ außerdem Koch, Internet-Recht, S. 958 sowie Kröger/Göers/Hanken, Internet für Juristen, S. 484.

[327] Davis, IPSec, S. 43.

[328] Schneider, MMR 1999, 571, 571; Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 83 ff.

[329] Vgl. hierzu auch Vorschlag der Kommission, S. 7/16, in welchem darauf verwiesen wird, dass es sich bei den Diensten der Informationsgesellschaft (im Sinne der Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG) um eine Vielzahl höchst unterschiedlicher Wirtschaftstätigkeiten handelt, die sich über das Netz abwickeln lassen.

[330] Vgl. auch Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 26.

[331] Sieber in: Hoeren/Sieber, Teil 1 Rn. 79; Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 26. Alle Protokolle des Internet sind in so genannten RFC beschrieben (zu RFC siehe S. 28 Fn. 100). Allgemein zu dem Begriff des Protokolls siehe auch Kröger/Göers/Hanken, Internet für Juristen, S. 482 sowie die Ausführungen auf S. 19 ff.

Angebot seitens eines Anbieters, Daten auf einem Server zum Abruf bereit zu stellen und mittels ftp zu übertragen, ist hingegen ein Online-Dienst, und zwar im Sinne einer wirtschaftlichen Tätigkeit, die im Internet erbracht wird.

So wird beispielsweise für das Übertragungsprotokoll ftp[332] vertreten, dass es sich um einen Teledienst oder Mediendienst handelt.[333] Sofern dies in der Allgemeinheit richtig ist, und damit Internet-Dienste Indikatoren für die rechtliche Einordnung von Online-Diensten sein können, könnte die rechtliche Prüfung dadurch wesentlich erleichtert werden. Zu prüfen ist, ob die im technischen Teil dargestellten Tunneling-Protokolle, welche wie ftp als Übertragungsprotokolle anerkannt sind,[334] ebenso Internet-Dienste darstellen und als Basis für die Einordnung von Dienstleistungen im VPN dienen können.

Die Internet-Dienste sind dementsprechend aufgrund ihrer Protokolle[335] gleichbedeutend mit Kommunikationslösungen zu sehen sind und ermöglichen, sämtliche elektronischen Dienstleistungen bzw. wirtschaftliche Tätigkeiten in elektronischer Form über das Internet abzuwickeln.[336] Die Internet-Dienste sind allesamt technischer Natur,[337] wobei die Online-Dienste-Anbieter diese technischen Möglichkeiten nutzen, um ihren Kunden den gewünschten Service anbieten zu können.[338] Internet-Dienste bilden somit die technische Basis von Online-Diensten.[339]

---

[332] Vgl. zu ftp S. 23, insbesondere Fn. 82.

[333] Spindler in: Roßnagel, Recht der Multimedia-Dienste, § 2 TDG Rn. 82 ff.; Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 83. Vgl. auch Holznagel in: Hoeren/Sieber, Teil 3.2 (bis zur 5. Ergänzungslieferung) Rn. 57 (Tabelle), der dort eine Einordnung als Teledienst vornimmt; siehe nunmehr aber Holznagel/Kibele in: Hoeren/Sieber, Teil 5, Rn. 68, die ftp als Mediendienst gemäß § 2 Abs. 2 Nr. 4 MDStV mit der Begründung qualifizieren, dass er an eine beliebige Öffentlichkeit gerichtet und damit Abrufdienst ist.

[334] Vgl. S. 34.

[335] Weitere Internet-Dienste wie Archie oder WAIS (siehe Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 13) werden auch als Programmsysteme bezeichnet, wobei jedoch ein Programm ebenfalls eine Folge von Anweisungen und Definitionen ist, die den Anwender in die Lage versetzen, Datenverarbeitungen durchzuführen, so dass es sich ebenso um ein technisches Werkzeug im Rahmen der Datenübertragung handelt (vgl. etwa Voss, Das große PC & Internet Lexikon 2007, S. 658).

[336] Vgl. Eichhorn, Internet-Recht, S. 20, der Internet-Dienste mit Kommunikationslösungen ausdrücklich gleichsetzt; siehe auch Schneider, MMR 1999, 571, 571; Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 83 ff.

[337] Siehe aber auch Holznagel in: Hoeren/Sieber, Teil 3.2 (bis zur 5. Ergänzungslieferung) Rn. 57 (Tabelle), der den Begriff Internet-Dienst auch auf Angebote wie Homebanking angewendet hat, nunmehr aber (siehe Holznagel/Kibele in: Hoeren/Sieber, Teil 5 Rn. 73 (Tabelle)) den Begriff „Inhalte-Dienste“ verwendet.

[338] Es muss zwar heutzutage das Vorhandensein von proprietären Online-Diensten oder Anbietern von Online-Diensten verneint werden. Es scheint jedoch durchaus legitim, davon

II. Mehrpersonenverhältnis

Entsprechend der unter I. entwickelten Begriffsdefinition eines Online-Dienstes ist daher im Rahmen einer datenschutzrechtlichen Prüfung in einem VPN zu beachten, welche Personen beteiligt und/oder betroffen sind.
Hierbei ist zu beachten, dass die Bezeichnungen wie „Nutzer“ oder „Betroffener“ auf eine identische Person zutreffen können, je nachdem welches Personenverhältnis betrachtet wird.

Die rechtlichen Betrachtungen gehen von den folgenden Begriffsdefinitionen aus:

1. Provider

Bei einer kombinierten Dienstleistung des in dieser Arbeit untersuchten Komplettpakets[340] VPN wird der Oberbegriff „Provider“ für denjenigen gewählt, der ein solches umfassendes Dienstangebot einem Kunden anbietet.

Überholt ist es, den Begriff „Internet-Provider“ lediglich auf den Internetzugangsanbieter (Access-Provider) zu beschränken.[341] Diese Begriffsbestimmung stammt noch aus den Anfängen des Internetzeitalters in Deutschland, das sich erst in den neunziger Jahren entwickelt hat.[342]

---

auszugehen, dass es proprietäre Internet-Dienste gibt. Denn wenn gemäß obiger Begriffsdefinition zugrunde gelegt wird, dass es sich bei Internet-Diensten um die technischen Möglichkeiten des Internet handelt, dann sind diese für das Internet aufgrund der technischen Struktur und der Eigentümlichkeit des Transportsystems des Internets gerade typisch und charakteristisch: Alle Dienste setzen auf das TCP/IP-Protokoll auf (vgl. Schneider, MMR 1999, 571, 571), so dass man in dieser Hinsicht von proprietär bzw. eigentümlich sprechen darf.
[339] Vgl. auch Beck-IuKDG-Engel-Flechsig, Glossar S. 830.
[340] Zum Komplettpaket siehe S. 4.
[341] So aber noch Voss in der 1. Auflage, Das große PC Lexikon, S. 439/605; Geis, Recht im eCommerce, Glossar S. 20/209 („Provider“ und „Service Provider“).
[342] Access Provider gibt es in Deutschland erst seit 1993, und zwar als aus zwei Forschungsprojekten an den Universitäten Dortmund und Karlsruhe die Eunet GmbH und die XLink GmbH entstanden sind. Geschäftsgegenstand war es, sowohl privaten Nutzern als auch Unternehmen den Internetzugang zu ermöglichen und dafür ein Entgelt zu erheben. Bis dato war es in Deutschland nur möglich, sich über die Universitäten Dortmund und Karlsruhe Zugang zum Internet zu verschaffen. Das Geschäftsmodell war durch die Liberalisierung des deutschen Telekommunikationsmarktes umsetzbar, da es nun möglich war, eigene Kapazitäten (Bandbreiten) auf den Leitungen der deutschen Telekom anzumieten und diese an die Kunden auf Basis der Internetprotokolle weiter zu vermieten (siehe hierzu Summa in: Holznagel/Nelles/Sokol, TKÜV, S. 23 sowie zur Entmonopolisierung Fn. 93 in dieser Arbeit).

Denn damals hatten die Provider lediglich eine einzige Aufgabe, die darin bestand, dafür Sorge zu tragen, dass der Rechner der Kunden über die Telefonleitung an das Internet angeschlossen werden konnte.[343]

Heutzutage stellt der Begriff „Internet-Provider“ den Oberbegriff für alle diejenigen dar, die irgendwie geartete Dienste im Internet anbieten.[344] So fallen ebenso Content-Provider, also Anbieter die Inhalte anbieten,[345] wie auch Presence Provider[346] bzw. Service Provider[347], also Anbieter, die ihren Kunden durch Unterstützung bei der Gestaltung von Internetseiten zu einem Webauftritt verhelfen, unter den Begriff des Providers bzw. Internet-Providers.[348] Ein einziger Provider kann heutzutage unterschiedliche Providertätigkeiten gleichzeitig wahrnehmen.[349]

Bei einem VPN wird sehr deutlich, dass der Begriff des reinen Zugangs-Providers bzw. Access-Providers nur dann passt, wenn ein Provider, wie beispielsweise T-Online, tatsächlich seinem Kunden allein an einem Standort einen Internetzugang bereit stellt, mit dem er selbständig seine Standorte

[343] Vgl. zur Geschichte des Internet auch Strömer, Online-Recht, S. 3/4.
[344] Vgl. Schneider, Verträge über Internet-Access, S. 89.
[345] Eichhorn, Internet-Recht, S. 43; teia (Hrsg.), Recht im Internet, S. 620; Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 50; Stögmüller in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 68; Schaar, Datenschutz im Internet, Rn. 305; Köhntopp/Köhntopp, CR 2000, 248, 250; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 12; Glatt, Vertragsschluss im Internet, S. 12; Martens/Schwarz-Gondek in: Bräutigam/Leupold, Glossar S. 1070 „Content-Provider“; Pelz in: Bräutigam/Leupold, B I. Rn. 44; Schneider, Verträge über Internet-Access, S. 94; Pankoke, Von der Presse- zur Providerhaftung, S. 170/171. Siehe zur Verantwortlichkeit von Content-Providern Stögmüller in: Spindler, Vertragsrecht der Internet Provider, Teil I Rn. 199 ff.
[346] Siehe zum „Presence Provider“ Eichhorn, Internet-Recht, S. 43; Koch, Internet-Recht, S. 4; Cichon, Internetverträge, Rn. 155 ff.; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 12; Schneider, Verträge über Internet-Access, S. 93 Fn. 454.
[347] Vgl. Sieber in: Hoeren/Sieber; Teil 1 Rn. 17; Stögmüller in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 68; Köhntopp/Köhntopp, CR 2000, 248, 250; Glatt, Vertragsschluss im Internet, S. 12; Martens/Schwarz-Gondek in: Bräutigam/Leupold, Glossar S. 1089 „Service-Provider“; Pelz in: Bräutigam/Leupold, B I. Rn. 44; Pankoke, Von der Presse- zur Providerhaftung, S. 171. Siehe zur Verantwortlichkeit von Service-Providern Stögmüller in: Spindler, Vertragsrecht der Internet Provider, Teil I Rn. 194 ff.
[348] Siehe zu den Begriffen von „Content- Service- oder Access-Provider“ auch Kloepfer, Informationsrecht, § 13 Rn. 24 ff. Diese Begrifflichkeiten sind durchgängig in der Literatur zu finden. Zum Teil werden über diese Provider hinaus weitere Typen aufgezählt, wie beispielsweise der Net-Provider (Schneider, Verträge über Internet-Access, S. 94), auch als Network-Provider bezeichnet (Sieber in: Hoeren/Sieber, Teil 1 Rn. 17), der als Betreiber oder Eigentümer von Leitungsverbindungen die physische Infrastruktur bereitstellt.
[349] Vgl. hierzu insbesondere auch Pelz in: Bräutigam/Leupold, B I. Rn. 45, der darauf verweist, dass ein Provider auch mehrere Funktionen, sprich unterschiedliche Providertätigkeiten gleichzeitig wahrnehmen kann; außerdem Spindler, CR 2004, 203, 203 mit der Feststellung, dass es ein Leitbild des Providervertrages kaum gibt, da in der Praxis eine Vielzahl von Leistungen miteinander kombiniert werden.

vernetzen kann.[350] Übernimmt der Provider zusätzlich das Management des Gateways und stellt die entsprechende Technik sowie den E-Mail-Dienst bereit, so zeigt sich, dass keiner der herkömmlichen Provider-Begriffe den Online-Dienst VPN in seiner Gesamtheit beschreiben vermag. Derjenige, der den Internetzugang bereitstellt und das Systemmanagement übernimmt, leistet mehr als ein reiner Access-Provider bzw. Internetzugangs-Provider.[351]

Dementsprechend empfiehlt sich ebenso für andere neue komplexe Online-Dienste, wie beispielsweise Application Service Providing[352] oder dem Angebot von Backup-Lösungen,[353] von den drei „klassischen“ Provider-Einteilungen Abstand zu nehmen, die, wie oben angesprochen, mit einem VPN kombiniert werden können.[354] Denn diese Begrifflichkeiten vermögen nicht die Leistungsvielfalt darzulegen bzw. erlauben keinen Rückschluss auf den eigentlichen Leistungsinhalt der angebotenen Dienste.
So ist ein Anbieter von Application Service Providing nicht (nur) im Sinne eines Content-Providers zu verstehen.[355] Zwar ist die eigentlich charakteristische Leistung des Application Service Providing, einem Nutzer per Fernzugriff die Benutzung von Anwendungssoftware zu erlauben.[356] Jedoch wird beim

---

[350] So etwa bei einem reinen Software-VPN, oder aber wenn der Kunde selbst das Systemmanagement bei einem kombinierten Hard- und Software-VPN übernimmt.
[351] Siehe beispielsweise das Angebot von T-Online unter „SecureVPN-Benutzerhandbuch“, insbesondere dort S. 239 sowie das Beispiel auf S. 49 in dieser Arbeit.
[352] Zum Application Service Providing siehe S. 74.
[353] Zum Angebot von Backup-Lösungen siehe S. 74 Fn. 313.
[354] Selbstverständlich soll dies nicht bedeuten, dass es beispielsweise nunmehr nicht mehr den Begriff Internetzugangs-Provider bzw. Access-Provider geben soll. Denn dort, wo die Begriffsbestimmung eine Einzelleistung zutreffend charakterisiert, ist auch die entsprechende Verwendung vorteilhaft. Es sollte lediglich vermieden werden, durch einschränkende Begriffsbildungen die Leistungsvielfalt von Diensten nicht mehr allumfassend beschreiben zu können, oder durch starre Begriffsbildung die gesetzliche Einordnung des Dienstes bereits im Vorfeld festzulegen (siehe hierzu die folgende Fn. 355).
[355] Zum einen impliziert der Begriff des Content-Providers, dass zwangsläufig das TDG oder der MDStV zur Anwendung gelangt (vgl. etwa Spindler in: Roßnagel, Recht der Multimedia-Dienste, § 5 TDG Rn. 53 ff.), obwohl strittig ist, ob Application Service Providing einen Teledienst (so Röhrborn/Sinhart CR 2001, 69, 74) oder einen Telekommunikationsdienst (siehe Bettinger/Scheffelt CR 2001, 729, 732) darstellt.
[356] Siehe S. 74 in dieser Arbeit sowie v.Westerholt/Berger, CR 2002, 81, 81, wobei die Software physikalisch auf dem Server des Anbieters verbleibt, wo der eigentliche Programmablauf erfolgt (Bettinger/Scheffelt CR 2001, 729, 733). Soll die Darstellung mittels des Browsers auf dem Bildschirm des Nutzers erfolgen, sind so genannte Java-Applets notwendig (zur Verwendung von Java-Applets bei ASP siehe Grützmacher, ITRB 2001, 59, 60). Diese enthalten einen bestimmten Code, der in einem HTML-Dokument integriert ist. Damit der Rechner des Nutzers die Anwendungssoftware lesen, nutzen bzw. bearbeiten kann, muss aus diesem Applet der konkrete Maschinencode erzeugt werden. Das Applet sorgt als eigenständiges Computerprogramm dafür, dass die Anwendungssoftware gestartet werden kann (vgl. hierzu Tanenbaum, Computernetzwerke, S. 880, der in einem Bildbeispiel darstellt, dass die Applets

Application Service Providing den Kunden oftmals darüber hinaus der Internetzugang sowie die Möglichkeit angeboten, die bearbeiteten Daten auf eigenen Servern (Rechnern) des Anbieters zu hosten[357] bzw. zu speichern,[358] insbesondere um die monatlichen Gebühren im Sinne eines Pauschalpreises abrechnen zu können.[359]
Daher würde der Begriff des Content-Providers den angebotenen Dienst nicht vollumfassend charakterisieren.

Ähnliches gilt für den Anbieter von Online-Backup-Lösungen. Denn hier ist der Anbieter weder Content Provider, da der Nutzer den Inhalt letztendlich selbst bereitstellt, noch ist der Anbieter einer Online-Backup-Lösung im herkömmlichen Sinne ein Presence Provider, der seinen Nutzern zum Webauftritt verhilft.[360]

Unter Berücksichtigung der gerade gemachten Ausführungen sowie der Auslegung des Begriffs „Online-Dienst" kann der Begriff „Provider" für jede Dienstleistung in jedwedem Anbieter-Nutzer-Verhältnis Anwendung finden, soweit es sich nicht um eine rein interne oder private Kommunikation handelt.[361] Zur besseren Abgrenzung bei der Prüfung der einzelnen Beteiligtenverhältnisse soll jedoch im Folgenden nur derjenige Anbieter als Provider bezeichnet werden, der die Dienstleistungen eines VPN kommerziell bzw. mit Gewinnabsicht anbietet.[362]

---

auf eine Website gestellt werden, um mit der Seite heruntergeladen zu werden. Nachdem die Seite geladen wurde, werden die Applets im Browser eingefügt).

[357] Zum Begriff des Hosting siehe Fn. 313.

[358] Vgl. auch Dück, ASP-Magazin, S. 22, 23. Grundsätzlich fällt auch das Web-Hosting unter den Begriff des Application Service Providing (Niedermeier/Damm, RDV 2001, 213, 213).

[359] Der Nutzer vermeidet so hohe Anschaffungskosten und kann die Nutzung punktgenau bzw. das Entgelt für die effektive Dauer der Softwarenutzung abrechnen (Röhrborn/Sinhart, CR 2001, 69, 69; Czychowski/Bröcker, MMR 2002, 81, 81). Durch die Leistungsbereitstellung „on demand" werden Tarifierungsmodelle möglich, welche den Nutzungspreis von Intensität oder Häufigkeit der Nutzung abhängig machen (Bettinger/Scheffelt, CR 2001, 729, 729).

[360] Denn die gespeicherten Daten sollen nicht öffentlich zugänglich gemacht werden, sondern vielmehr verborgen bleiben und nur dem Nutzer zur Verfügung stehen.

[361] Vgl. Erwägungsgrund 18 der E-Commerce-Richtlinie (Fn. 27), der die Verwendung elektronischer Post oder gleichwertiger individueller Kommunikation durch natürliche Personen außerhalb ihrer geschäftlichen oder beruflichen Tätigkeit nicht als Dienst der Informationsgesellschaft einordnet. Diese Ausnahme gilt auch innerhalb dieser Arbeit, da Datenschutz innerhalb rein privater oder familiärer Tätigkeiten keine Anwendung findet und daher nicht zu untersuchen ist (vgl. auch § 1 Abs. 2 Nr. 3 BDSG).

[362] Vgl. hierzu auch Härting, CR 2001, 37, 37, der ausführt, dass mit dem englischen Begriff des „Providers" nur Unternehmen gemeint sind, die dem Kunden die Voraussetzungen für eine aktive oder auch nur passive Nutzung des Internets bereitstellen.

Soweit das TKG zur Anwendung gelangt, ist demzufolge stets geschäftsmäßiges Handeln gemäß § 3 Nr. 10 TKG bzw. die Eigenschaft als Diensteanbieter gemäß § 3 Nr. 6 TKG gegeben ist, da kommerzielles und auf Gewinnerzielung ausgerichtetes Handeln, zwangsläufig bzw. mindestens geschäftsmäßig ist, also eine auf Dauer angelegte Tätigkeit, die eine gewisse Nachhaltigkeit aufweist.[363]

2. VPN-Auftraggeber

Als VPN-Auftraggeber wird derjenige bezeichnet, der mit einem Provider im Hinblick auf die Realisierung eines Internet-VPN bzw. der Vernetzung seiner Standorte und der Einrichtung des E-Mail-Service einen Vertrag abgeschlossen hat. Er ist insoweit Kunde[364] des Providers und kann ebenso Anbieter[365] von Diensten im Verhältnis zu Nutzern des VPN sein.

3. Nutzer (Mitarbeiter, Externer, E-Mail-Kommunikationspartner)

Unter Nutzer[366] eines VPN sind diejenigen Personen oder Personengemeinschaften zu verstehen, denen der VPN-Auftraggeber ein VPN zur Nutzung bereitstellt und denen er damit den Zugriff auf sein Unternehmensnetzwerk gestattet.[367]
Diese in das VPN eingebundenen Personen können sowohl Mitarbeiter des VPN-Auftraggebers als auch Externe sein, wie beispielsweise Lieferanten. Eingangs wurde in diesem Zusammenhang bereits erwähnt, dass ebenso in der

---

[363] Vgl. zur Geschäftsmäßigkeit Ehmer in: TKG-Kommentar (2. Auflage), § 87 TKG Rn. 13 ff.; Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 18; Zerres in: Scheurle/Mayen, TKG-Kommentar, § 85 TKG Rn. 22 ff.; Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 87 TKG(1998), Band 1, Rn. 8.
[364] Siehe auch § 3 Nr. 20 TKG, wonach der Begriff „Teilnehmer“ die Kunden des Diensteanbieters meint, und zwar die natürlichen oder juristischen Personen, die mit einem Anbieter von Telekommunikationsdiensten einen Vertrag über die Bereitstellung derartiger Dienste geschlossen haben.
[365] Der Begriff des Providers soll im Übrigen, wie gerade dargestellt, nur verwendet werden, sofern es sich um einen kommerziellen Anbieter handelt, dessen Geschäftszweck in der Erbringung von Online-Diensten besteht.
[366] Nutzer meint gemäß § 3 Nr. 14 TKG jede natürliche Person, die einen Telekommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben. Gemäß § 3 Nr. 2 TDG ist ein Nutzer jede natürliche oder juristische Person, die zu beruflichen oder sonstigen Zwecken Teledienste in Anspruch nimmt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.
[367] Siehe oben die Bildbeispiele S. 2/44 ff.

Beziehung zwischen VPN-Auftraggeber und Lieferanten ein Interesse an einem VPN besteht.[368]

Im Hinblick auf den Zusatzdienst E-Mail wird als Nutzer zum einen der Mitarbeiter des VPN-Auftraggebers bezeichnet, der diesen Dienst durch Einrichtung eines eigenen E-Mail-Accounts vom VPN-Auftraggeber zur eigenen Nutzung bereitgestellt bekommt.
Da der VPN-Auftraggeber regelmäßig nur für seine Mitarbeiter einen E-Mail-Account einrichten wird, kommen hier lediglich seine Arbeitnehmer und freie Mitarbeiter als Nutzer des E-Mail-Dienstes in Betracht, aber nicht beispielsweise Lieferanten des VPN-Auftraggebers.
Zum anderen soll von dem Begriff „Nutzer" aber auch derjenige erfasst sein, der mit dem VPN-Auftraggeber oder dem Mitarbeiter des VPN-Auftraggebers in E-Mail-Korrespondenz steht. Denn derjenige, der eine E-Mail empfängt, ist gleichermaßen ein Nutzer einer Dienstleistung, da er einen E-Mail-Dienst bzw. ein Angebot zur Kommunikation insoweit ebenfalls nutzt und in Anspruch nimmt. Er hat sich durch die Bereithaltung eines E-Mail-Accounts willentlich und aktiv in die allgemeine Kommunikation per Internet als Beteiligter eingebracht, da er einen E-Mail-Account bereithält.
Der Begriff des Nutzers kann dementsprechend unterschiedliche Bedeutungen haben, was im Verlauf dieser Arbeit stets hinreichend deutlich gemacht wird.

Diese Begriffsbestimmung entspricht im Übrigen der in dieser Arbeit entwickelten Definition, dass es sich bei einem Dienst allein um eine wirtschaftliche Tätigkeit handelt, die unabhängig von einem festen Anbieter und festen Nutzer zu betrachten ist.[369]

[368] Siehe S. 2.
[369] Siehe oben S. 71 ff.

4. Betroffener

Der Begriff der „Betroffenen“ bezeichnet diejenigen Personen, deren Daten innerhalb eines Online-Dienstes übertragen werden, ohne dass sie diese Übertragung aktiv durch Ingangsetzen eines Kommunikationsvorganges selbst veranlasst haben.[370]
Dies ist bei dem hier zu untersuchenden VPN etwa möglich, wenn ein Nutzer (z.B. Telearbeiter, Tochterunternehmen, Externer) auf den Server der Firmenzentrale zugreift, auf welchem Kunden- oder Mitarbeiterdaten gespeichert sind.
Beim Zusatzdienst E-Mail kann eine versendete E-Mail Daten eines Kunden oder Mitarbeiters enthalten, die insoweit zu Betroffenen werden.[371]

Zuzugeben ist, dass die Grenzen zwischen den Begriffsdefinitionen „Nutzer“ und „Betroffener“ fließend sind. In dieser Arbeit soll jedoch der Begriff des Betroffenen nur für Personen verwendet werden, die nicht aktiv am Kommunikationsvorgang beteiligt sind, aber deren Daten dennoch während dieses Kommunikationsvorganges durch die Übertragung innerhalb des VPN oder per E-Mail, insbesondere von VPN-Auftraggeber zu dem Nutzer des VPN und umgekehrt, verarbeitet werden.

Im Übrigen wird auch bezüglich des Begriffs „Betroffener“ im Verlaufe dieser Arbeit stets deutlich gemacht, wer der jeweilige Betroffene ist, und bei der Abgrenzung zwischen, Nutzer und Betroffener eines Dienstes soll insgesamt die Frage nach der aktiven Beteiligung am Internetkommunikationsvorgang im Vordergrund stehen.

[370] Siehe auch die Ausführungen in Fn. 361, aus denen sich ergibt, dass eine Person dann nicht Betroffener sein kann, sofern es sich nicht um einen Dienst der Informationsgesellschaft, sondern allein um eine rein private Tätigkeit handelt.
[371] Siehe ebenso die Bildbeispiele auf S. 2/44 ff.

III. Datenschutz und Datensicherheit

Um den Datenschutz innerhalb eines VPN prüfen zu können, sind die datenschutzrechtlichen Voraussetzungen einer Datenverarbeitung darzulegen. Hierzu wird im Folgenden eine Übersicht notwendiger Prüfungspunkte dargestellt, wobei ebenso auf die Schranken des Datenschutzes aufgrund staatlicher Auskunfts- und Überwachungsmaßnahmen eingegangen wird.

1. Grundlagen

Für das Verständnis dieser Arbeit sind die nachfolgenden zwei Grundannahmen von Bedeutung.

a. Dienstorientierte Betrachtungsweise im Mehrpersonenverhältnis

In dieser Arbeit ist nicht allein die Trennung zwischen Transport- und Inhaltsebene in einem Online-Dienst von Bedeutung.[372] Die datenschutzrechtliche Betrachtung konzentriert sich ebenso darauf, das Komplettpaket VPN in jedwedem Personenverhältnis in seine einzelnen Dienstleistungen aufzuspalten.[373] Innerhalb dieser Personenverhältnisse werden diese „Einzel-Dienstleistungen“ betrachtet und rechtlich als Telekommunikationsdienstleistungen gemäß § 3 Nr. 24 TKG oder Teledienste gemäß § 2 Abs. 1 TDG eingeordnet. Dies soll zum einen eine datenschutzrechtliche Aussage gleichermaßen für den Fall ermöglichen, sofern mehrere Transportebenen innerhalb eines VPN vorliegen sollten. Zum anderen stellt diese Betrachtung die Grundlage für die Untersuchung dar, ob sich die rechtliche Einordnung von Dienstleistungen in Abhängigkeit vom (jeweiligen) untersuchten Personenverhältnis ändern kann.

Die Abgrenzung zwischen Telekommunikationsdienstleistung gemäß § 3 Nr. 24 TKG (Transportebene) und Teledienst gemäß § 2 Abs. 1 TDG (Inhaltsebene) wird anhand der Frage vertieft behandelt, ob die dem VPN zugrunde liegende

[372] Siehe zur funktionalen Betrachtungsweise S. 66 ff.
[373] Siehe zur dienstorientierten Betrachtungsweise im Mehrpersonenverhältnis S. 74 ff.

Technik für die rechtliche Einordnung einer Einzelleistung des kombinierten Online-Dienstes „VPN“ herangezogen werden kann.[374]

b. Betrachtungsgrenzen

In dieser Arbeit wird ausschließlich die Datenverarbeitung innerhalb eines deutschlandweiten VPN behandelt. Eine Prüfung grenzüberschreitender Fragestellungen würde die in nachfolgenden Ausführungen dargestellten zusätzlichen Rechtsfragen aufwerfen, deren Beantwortung im Rahmen dieser Arbeit zu umfassend wäre. Denn zusätzlich zu den bereits behandelten rechtlichen Problemen müsste eine ausführliche Auseinandersetzung mit den Rechtsvorschriften des § 4 b BDSG und § 4 c BDSG erfolgen, die den Bereich der internationalen Datenverarbeitung regeln. Dabei spielt beim grenzüberschreitenden Datenverkehr in Drittländer (außerhalb der EU) stets das „angemessene Schutzniveau“ eine große Rolle, wie sich aus den folgenden Ausführungen ergibt.[375]

aa. Datenverarbeitung außerhalb der EU

Die (daten)übermittelnde Stelle muss gemäß § 4 b Abs. 3 BDSG prüfen, ob ein angemessenes Datenschutzniveau in den Ländern außerhalb der EU vorliegt.[376] Ein zulässige Datenverarbeitung und ein angemessenes Schutzniveau liegt zwar beim internationalen Datenverkehr in Drittländer grundsätzlich vor, wenn zwischen den verantwortlichen Stellen die von der EU-Kommission am 15.06.2001 und am 27.12.2001 verabschiedeten Standardvertragsklauseln zur Gewährleistung der Schutzinteressen der Betroffenen vereinbart werden.[377] Dies gilt allerdings nur bei wortgetreuer Übernahme der Standardvertragsklauseln, da geringfügige Abweichungen

[374] Siehe hierzu im Folgenden auf S. 305 ff.
[375] Siehe zu der Frage des „angemessenen Datenschutzniveaus“ auch Däubler, Gläserne Belegschaften?, Rn. 501 ff.
[376] Vgl. auch Tinnefeld, NJW 2001, 3078, 3082. Däubler, NZA 2001, 874, 879.
[377] ABl. EG Nr. L 181 v. 14.07.2001, S. 19-31 und ABl. EG Nr. 6 L v. 10.01.2002, S. 52-62 letztere neugefasst durch Entscheidung der Kommission vom 27.12.2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (ABl. EG Nr. L 385 v. 29.12.2004, S. 74-84. Siehe hierzu auch Gola/Schomerus, BDSG, § 4b BDSG Rn. 16 sowie Räther/Seitz, MMR 2002, 520 ff. Zur Kritik an der Vertragslösung, allerdings noch vor Verabschiedung der Standardvertragsklauseln, siehe Geis, NJW 1997, 288, 289 ff.

ebenso zur Genehmigungspflicht nach § 4 c Abs. 2 BDSG führen.[378] Es wäre daher eine inhaltliche Beschäftigung mit den Standardvertragsklauseln gefordert, da diese nicht kritiklos betrachtet werden.[379]
Jedes Unternehmen und jeder Unternehmerverband hat darüber hinaus die Möglichkeit, eigene Standardvertragsklauseln zu entwerfen und der Kommission zur Anerkennung vorzulegen,[380] so dass hier außerdem der Gesichtspunkt der inhaltlichen Ausgestaltung dieser vertraglichen Regelungen eine große Rolle spielen würde.

In diesem Zusammenhang wären nicht nur Bereiche des allgemeinen Zivilrechts, etwa des Internationalen Privatrechts, betroffen, sondern gleichermaßen die Frage, (wie) Datenschutz in der Praxis vollstreckt werden kann. Welche Konsequenz ergibt sich, wenn der Datenverarbeiter (beispielsweise mit Sitz in Armenien) die vertraglich zugesicherten Datenschutzkontrollen verweigert? Der Schwerpunkt der Beantwortung dieser Fragen sollte dementsprechend darauf liegen, ob vertragliche Regelungen den Datenschutz tatsächlich in angemessener Form sicherstellen können.

In die gleiche Richtung zielt das (rechtspolitische) Problem, inwieweit ein „blinder" Datenverkehr in Länder gerechtfertigt ist, für welche die EU-Kommission festgestellt hat, dass ein angemessenes Datenschutzniveau gewährleistet ist.[381] Hierzu zählen Datenempfänger, die ihren Sitz in Ungarn, Schweiz oder Kanada haben bzw. wie die USA am Safe-Harbor-Programm teilnehmen.[382]
Der Umgang mit Ländern, die sich nicht den Safe-Harbor-Prinzipien unterworfen haben, oder die Frage, ob zur Erzielung eines besseren Datenschutzniveaus (zusätzlich zu den Safe-Harbor-Regelungen) einzelne Normen der Standardvertragsklauseln vereinbart werden sollten, bedarf gleichermaßen einer vertieften Auseinandersetzung mit den Safe-Harbor-Regelungen einerseits sowie mit den datenschutzgesetzlichen Regelungen der

---

[378] Räther/Seitz, MMR 2002, 520, 522.
[379] Vgl. etwa Räther/Seitz, MMR 2002, 520. 525/526 zu den Haftungsklauseln im Rahmen der Funktionsübertragung.
[380] Vgl. Räther/Seitz, MMR 2002, 520. 522.
[381] Vgl. Räther/Seitz, MMR 2002, 520. 520.
[382] Zu den Safe-Harbor-Regelungen siehe auch die Ausführungen von Räther/Seitz, MMR 2002, 425, 427 ff.

einzelnen Länder andererseits.

Des Weiteren müsste eine datenschutzrechtliche Prüfung des grenzüberschreitenden Datenverkehrs den so genannten Code of Conduct berücksichtigen. Dieser beinhaltet neben den Vertragsklauseln eine weitere Möglichkeit, das angemessene Schutzniveau im datenimportierenden Land durch verbindliche Unternehmensregelungen sicherzustellen.[383]
Der Code of Conduct stellt jedoch keine Universallösung für einen ungehinderten Datenaustausch dar.[384] Diesbezüglich taucht außerdem die Frage auf, ob gegebenenfalls mehrere Codes of Conduct für unterschiedliche Datenarten (etwa Personaldaten, Kundendaten) verwendet werden sollten.[385] Damit ist ebenso eine gründlichere datenschutzrechtliche Stellungnahme zu Möglichkeiten und Grenzen eines solchen Code of Conducts angezeigt.

Abschließend muss darüber hinaus auf die Problematik des Zugriffs staatlicher Sicherheitsbehörden auf die exportierten Daten hingewiesen werden, die datenschutzrechtliche Belange in besonderem Maße berühren.[386]

bb. Datenverarbeitung innerhalb der EU

Die Datenverarbeitung innerhalb der EU kommt ebenso wenig mit einer verkürzten Darstellung datenschutzrechtlicher Fragestellungen aus.
Gemäß § 4 b Abs. 1 BDSG in Verbindung mit Artikel 1 Abs. 2 EU-Datenschutz-Richtlinie[387] ist die Datenverarbeitung innerhalb der EU aufgrund des ausreichenden Datenschutzniveaus zwar ohne weiteres zulässig ist. Dennoch muss bei der Umsetzung des VPN gemäß § 1 Abs. 5 BDSG festgestellt werden, welches Datenschutzrecht eines Mitgliedstaates der EU im

---

[383] Siehe hierzu auch Fleck, BB 2003, 306, 307.
[384] Vgl. Räther/Seitz, MMR 2002, 520. 528.
[385] Vgl. Räther/Seitz, MMR 2002, 520. 527.
[386] Siehe hierzu Dix/Gardain, DuD 2006, S. 343, 346 unter Verweis auf die Entscheidung der Europäischen Kommission und des Rates, Flugpassagierdaten sämtlicher Reisender in die USA auf Vorrat übermitteln zu lassen.
[387] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Binnenmarkt jeweils anzuwenden ist.[388] Gemäß Art. 17 Abs. 3 zweiter Spiegelstrich der EU-Datenschutz-Richtlinie[389] findet beispielsweise bei den sicherzustellenden technischen und organisatorischen Maßnahmen(die im deutschen Recht in § 9 BDSG geregelt sind) das Recht des datenverarbeitenden Unternehmens Anwendung. Eine vollumfängliche datenschutzrechtliche Prüfung müsste daher beinhalten, inwieweit eine dem § 9 BDSG entsprechende ausländische Rechtsvorschrift von § 9 BDSG abweichende oder sogar konkretere Vorgaben bezüglich der technischen und organisatorischen Maßnahmen enthält. So sollte zumindest festgestellt werden können, ob die Interessen des Auftraggebers durch die gesetzlich normierten Maßnahmen bereits vollumfänglich abgebildet sind, oder ob die Notwendigkeit besteht, Sicherheitsmaßnahmen, wie beispielsweise Verschlüsselung von Daten, einzelvertraglich zu regeln. Grundsätzlich wäre auch denkbar, dass die gesetzlichen Regelungen des EU-(Aus)landes einen strengeren und konkreteren Maßstab beinhalten als die Regelung des § 9 BDSG, der sich im Wesentlichen am Grundsatz der Verhältnismäßigkeit orientiert.[390]

Findet die Datenverarbeitung nicht in Deutschland, sondern in einem EU-Land statt, müsste daher das Datenschutzgesetz dieses EU-Landes zur näheren Prüfung herangezogen.[391] Außerdem müsste entsprechend der oben angestellten Überlegungen zur Datenverarbeitung in EU-Drittländern berücksichtigt werden, welche vertraglichen Regelungen gegebenenfalls zusätzlich erforderlich sein könnten.

[388] Dolderer/v.Garrel/Müthlein/Schlumberger, RDV 2001, 223, 229/232. Siehe zur Privilegierung der Datenübermittlung in das EU-Ausland auch Däubler, NZA 2001, 874, 879.

[389] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[390] Vgl. zur Verhältnismäßigkeit Ernestus in: Simitis, BDSG-Kommentar, § 9 BDSG Rn. 23 ff.

[391] Vgl. etwa am Beispiel der Niederlande, dass die datenschutzrechtliche Gesetzgebung auf eine Vielzahl von allgemeinen und auf spezielle Bereiche bezogene Gesetze verteilt ist (siehe hierzu Spindler/Börner, E-Commerce-Recht in Europa und den USA, S. 741 ff.).

cc. Fazit

Insgesamt muss für eine aussagefähige Stellungnahme die Rechtsproblematik der Datenverarbeitung in einem grenzüberschreitenden VPN vertieft behandelt werden, so dass sich die rechtliche Sicht in dieser Arbeit auf die Datenverarbeitung in Deutschland beschränken muss.[392]

Mögliche Lösungen bezüglich der Datenverarbeitung im internationalen Bereich müssen daher gesondert ausgeführt werden. Ein Vorschlag wäre in diesem Zusammenhang in rechtspolitischer Hinsicht zu diskutieren, ob die oben dargestellten Problemfelder zu einem (freiwilligen) Verzicht eines Unternehmens zur Verlagerung der Datenverarbeitung in Drittländer führen müssen – selbst wenn diese grundsätzlich gesetzlich zulässig ist.
Es kann ebenso über mögliche Gesetzesänderungen nachgedacht werden. Für Daten, die dem Fernmeldegeheimnis unterliegen, schließt beispielsweise § 92 TKG eine Verarbeitung in Drittländern ausdrücklich aus. Dieser Ansatzpunkt könnte bei der Problemlösung insoweit verfolgt werden, indem zusätzliche Datenkategorien gebildet und Länder aufgezählt werden, für die ein Verzicht in Betracht kommen kann. Beispielsweise ist das Verarbeiten von (ausschließlich) E-Mail-Adresse und Nutzername weit weniger problematisch als das Verarbeiten von vollständigen Adressdaten und der Kaufhistorie eines Kunden in einem EU-Drittland.
Die Auflistung bestimmter Länder kann sich natürlich schwierig gestalten. Eine Möglichkeit bestünde jedoch darin, dass sich auf Bundesebene (innerhalb eines Ministeriums oder Bundesamtes) eine Kommission mit diesen Fragen beschäftigen könnte. Eine solche Kommission könnte darüber hinaus beispielsweise Unternehmen (anonym) befragen, welche Erfahrungen diese mit Drittländern hatten und welche Schwierigkeiten in der Praxis aufgetaucht sind.

[392] Einen Überblick zu kollisionsrechtlichen Fragen des Vertragsrechts sowie zur Datenschutzgesetzgebung in Europa und den USA bietet das Buch von Spindler/Börner, E-Commerce-Recht in Europa und den USA.

2. Zulässigkeit der Datenverarbeitung, -erhebung und -nutzung personenbezogener Daten

Die folgenden Ausführungen geben einen Überblick über Datenverarbeitungsregelungen der in dieser Arbeit einschlägigen Datenschutzgesetze. Im Einzelnen sind dies die Vorschriften des BDSG, der §§ 91 ff. TKG sowie des TDDSG.

a. Bundesdatenschutzgesetz (BDSG)

Bevor auf die Definition von personenbezogenen Daten und die Verarbeitungstatbestände des BDSG eingegangen wird, soll zunächst das Exklusivitätsverhältnis zwischen den Regelungen des BDSG einerseits sowie den Regelungen des TKG und TDDSG andererseits dargestellt werden.

aa. Exklusivitätsverhältnis

Das TKG regelt detailliert den Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten, das TDDSG bezieht sich auf diejenigen Daten, die dem Nutzer die Nachfrage nach Telediensten ermöglichen.[393]

Darüber hinaus sind aber ebenso die Regelungen des Bundesdatenschutzgesetz (BDSG) von Bedeutung,[394] die Anwendung finden, sofern in TKG oder TDDSG keine vorrangigen Regelungen enthalten sind.[395]

Damit wird das Exklusivitätsverhältnis zwischen BDSG und TKG bzw. TDDSG verdeutlicht und impliziert, dass die Erlaubnistatbestände des TDDSG und der §§ 91 ff. TKG abschließend sind und nicht ergänzend auf allgemeine

[393] Vgl. Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 111/114, der darüber hinaus auf den MDStV Bezug nimmt.
[394] Zum Bundesdatenschutzgesetz siehe Fn. 26.
[395] Siehe Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDDSG Rn. 60). Vgl. auch Richter, Datenschutzrechtliche Aspekte beim Tele- bzw. Homebanking, S. 138; Rasmussen, CR 2002, 36, 37 sowie Fechner, Medienrecht, Rn. 453, die im Zusammenhang mit dem TDDSG auf dessen Vorrang gegenüber dem BDSG hinweisen).

Erlaubnistatbestände -wie beispielsweise § 28 BDSG- zurückgegriffen werden kann.[396]

Dieses Exklusivitätsverhältnis ergibt sich ebenso aus § 1 Abs. 3 BDSG sowie § 1 Abs. 2 TDDSG. Letzterer regelt, dass die Regelungen des allgemeinen Datenschutzrechts Anwendung finden, wenn und soweit das TDDSG nichts anderes bestimmt. Die Bestimmungen des BDSG gelten insoweit subsidiär.[397] § 91 TKG enthält zwar keine der § 1 Abs. 2 TDSV entsprechende Regelung, aus der sich die Subsidiarität unmittelbar ergibt. Der Subsidiaritätsgedanke ergibt sich aber mittelbar aus dem TKG, etwa aus § 93 S. 4 TKG oder § 95 Abs. 3 TKG, und unmittelbar aus § 1 Abs. 3 BDSG.[398]

bb. Definition der personenbezogenen Daten

Die Definition von personenbezogenen Daten liefert das Bundesdatenschutzgesetz (BDSG).[399]
Gemäß § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
Personenbezogen sind die Daten im Sinne von Einzelangaben,[400] die sich auf eine bestimmte oder bestimmbare[401] natürliche Person beziehen.[402]

---

[396] Siehe Bundestag-Drucksache 14/6098, S. 29. Vgl. hierzu auch Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 137; Beckschulze, DB 2003, 2777, 2780; Nägele/Meyer, K&R 2004, 312, 313; Weißnicht, MMR 2003, 448, 450.

[397] Gemäß § 1 Abs. 2 TDDSG können die Regelungen des allgemeinen Datenschutzrechts (beispielsweise die Begriffbestimmungen des § 3 BDSG, der Grundsätze der Datenvermeidung nach § 3a BDSG sowie über die Regelungen der Aufsicht nach § 38 BDSG) Anwendung finden, wenn und weil das TDDSG nichts anderes bestimmt.

[398] Nach § 1 Abs. 2 TDSV haben die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten – insbesondere das BDSG – Anwendung gefunden, soweit die TDSV nichts anderes bestimmt hat (siehe auch Gola/Klug, Grundzüge des Datenschutzrechts, S. 201 mit dem Hinweis (zur damals geltenden TDSV), dass die Vorschriften der TDSV als bereichsspezifische Regelungen den allgemeinen Datenschutzregelungen des BDSG vorgehen.).

[399] Vgl. Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 101.

[400] Einzelgaben sind Informationen, die sich auf eine einzelne natürliche Person beziehen und geeignet sind, einen Bezug zu ihr herzustellen, vgl. Gola/Schomerus, BDSG, § 3 BDSG Rn. 3; Schulz in: Roßnagel, Recht der Multimedia-Dienste, § 1 TDDSG Rn. 28; Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 279. Eine beispielhafte Aufzählung der Einzelangaben über persönliche und sachliche Verhältnisse findet sich ebenso bei Steckler, Grundzüge des IT-Rechts, S. 68.

[401] Vgl. Ehmann/Helfrich, EG-Datenschutzrichtlinie, Einleitung Rn. 1, mit dem Hinweis, dass sich zur Auslegung der unbestimmten Rechtsbegriffe der Bestimmtheit bzw. Bestimmbarkeit der Text der EG-Datenschutzrichtlinie heranziehen lässt.

Ersteres ist der Fall, wenn die Daten mit dem Namen des Betroffenen verbunden sind oder sich aus dem Inhalt bzw. dem Zusammenhang der Personenbezug unmittelbar herstellen lässt.[403] Dies können z.B. Name, Ausweisnummer, Versicherungsnummer, Telefonnummer darstellen.[404] Die Daten sind schon dann personenbezogen, wenn sie sich mit dem Namen des Betroffenen (auf welchem Wege auch immer) verbinden lassen.[405]

Ist dies nicht der Fall sind die Daten nur dann personenbezogen, wenn der Betroffene bestimmbar ist.[406] Für diese Bestimmbarkeit kommt es auf die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle an. Sie muss den Bezug mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand durchführen können, um die Bestimmbarkeit zu bejahen.[407]
Dies bedeutet, dass dieselben Daten für den einen anonym und für den anderen der betroffenen Person zuordbar sein können,[408] so dass der Personenbezug insoweit relativ ist.[409]

cc. Verarbeitung personenbezogener Daten

Die Zulässigkeit der Verarbeitung von personenbezogenen Daten ergibt sich aus § 4 Abs. 1 BDSG. Danach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig,[410] soweit dieses Gesetz oder eine

---

[402] Vgl. Gola/Schomerus, BDSG, § 3 BDSG Rn. 9. Vgl. auch Wegel, Presse und Rundfunk im Datenschutz, S. 24 und den dortigen Ausführungen, dass Daten von juristischen Personen nur dem Datenschutzrecht unterfallen, wenn ein Personenbezug erkennbar ist.
[403] Gola/Schomerus, BDSG, § 3 BDSG Rn. 9; Schulz, Die Verwaltung 1999, 137, 163.
[404] Gola/Schomerus, BDSG, § 3 BDSG Rn. 3; Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 279.
[405] Steding, BB 2001, 1693, 1698.
[406] BGH, NJW 1991, 568, 570; Gola/Schomerus, BDSG, § 3 BDSG Rn. 9; Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 20 ff.
[407] Gola/Schomerus, BDSG, § 3 BDSG Rn. 9; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 91; Schulz, Die Verwaltung 1999, 137, 163; Schaffland/Wiltfang, BDSG, § 3 BDSG Rn. 17; Schulz in: Roßnagel, Recht der Multimedia-Dienste, § 1 TDDSG Rn. 28; Schneider, Handbuch des EDV-Rechts, Teil B Rn. 179; Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 54.
[408] Gola/Schomerus, BDSG, § 3 BDSG Rn. 9; Roßnagel/Scholz, MMR 2000, 721, 723.
[409] Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 33; Schulz, Die Verwaltung 1999, 137, 163; Roßnagel/Scholz, MMR 2000, 721, 723; Gola/Schomerus, BDSG, § 3 BDSG Rn. 9.
[410] Vgl. Roßnagel in: Roßnagel, Handbuch Datenschutzrecht, 1 Rn. 30, Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2 Rn. 92, Gola/Schomerus, BDSG, § 1 BDSG Rn. 22, die insgesamt darauf verweisen, dass die Dreiteilung in Erhebung, Verarbeitung und Nutzung nicht

andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.[411] Die Einwilligung ist hierbei in § 4a BDSG geregelt. Gemäß der Vorgaben Artikel 2 h der Richtlinie 95/46/EG[412] bedeutet Einwilligung der betroffenen Person jede Willensbekundung, die ohne Zwang für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.[413] Die entsprechende Umsetzung in § 4a Abs. 1 S. 3 BDSG beinhaltet, dass die Einwilligung dann nicht der Schriftform bedarf, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

§ 3 Abs. 3 BDSG regelt die Erhebung von Daten und meint damit das Beschaffen von Daten über den Betroffenen als Vorphase für die spätere Datenverarbeitung und Datennutzung,[414] wobei die Verarbeitung gemäß § 3 Abs. 4 BDSG in fünf unterschiedliche Verarbeitungsphasen unterteilt ist, und das Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten umfasst.[415] Unter Nutzung von Daten gemäß § 3 Abs. 5 BDSG ist jede Verwendung von personenbezogenen Daten zu verstehen, soweit es sich nicht um Verarbeitung handelt, und bildet insofern einen Auffangtatbestand.[416]

---

zeitgemäß und unglücklich gewählt ist, insbesondere unter Verweis auf ein modernes Datenschutzrecht.

[411] Siehe aber auch Globig in: Roßnagel, Handbuch Datenschutzrecht, 4.7 Rn. 36, der die Ansicht vertritt, dass die Erhebung und Nutzung nicht vom Wortlaut des § 4 Abs.1 BDSG erfasst, aber das in § 4 Abs. 1 BDSG enthaltene „Verbot mit Erlaubnisvorbehalt“ aufgrund der Eingriffsqualität von Datenerhebung und Nutzung dennoch auch für diese Phasen des Umgangs mit Daten gilt.

[412] Vgl. hierzu Fn. 30.

[413] Siehe zur Freiwilligkeit der Einwilligung Wedde, DuD 2004, 169, 172. Siehe außerdem Däubler, NZA 2001, 874, 876 mit dem Hinweis, dass eine Einwilligung nur dann rechtfertigende Wirkung entfalten kann, wenn sie „auf der freien Entscheidung“ des Betroffenen beruht. Vgl. Wiese, RdA 1986, 120, 127 zur Nichtigkeit der Einwilligung (im Arbeitsverhältnis) gemäß § 138 BGB bei fehlender Freiwilligkeit. Gola/Schomerus, BDSG, § 4a BDSG Rn. 6 verweisen darauf, dass die Einwilligung ohne Zwang erfolgen muss. Vgl. außerdem Anmerkung Linnenkohl/Schütz zu BAG, RDV 1987, 129, 134 (noch zu § 3 BDSG a.F.) mit dem Hinweis, dass der Eingriff in das Persönlichkeitsrecht verlangt, dass entweder eine Einwilligung oder die gesetzlichen Erlaubnistatbestände (als allgemeine Zulässigkeitsvoraussetzungen für die Verarbeitung der personenbezogenen Daten) vorliegen müssen.

[414] Vgl. Gola/Schomerus, BDSG, § 3 BDSG Rn. 24 sowie§ 4 BDSG Rn. 18; Schaffland/Wiltfang, BDSG, § 3 BDSG Rn. 195; Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 101; Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2 Rn. 35; Schneider, Handbuch des EDV-Rechts, Teil B Rn. 188.

[415] Siehe hierzu Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2 Rn. 55 ff. Auf einzelne, in dieser Arbeit relevante Phasen und Definitionen der Datenverarbeitung wird im Übrigen im Verlaufe der Arbeit eingegangen.

[416] Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2 Rn. 86; Schaffland/Wiltfang, BDSG, § 3 BDSG Rn. 106; Gola/Schomerus, BDSG, § 3 BDSG Rn. 42.

Eine Rechtsvorschrift im BDSG, die die Datenerhebung-, Datenverarbeitung oder Datennutzung erlaubt, und die in dieser Arbeit einschlägig ist, ist § 28 BDSG.
Im Sinne dieser Regelung kann die Datenerhebung, Datenverarbeitung und Datennutzung für die Erfüllung eigene Zwecke zulässig sein, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichem Vertrauensverhältnisses mit dem Betroffenen dient (§ 28 Abs. 1 Nr. 1 BDSG),oder soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist (§ 28 Abs. 1 Nr. 2 BDSG) oder wenn die Daten allgemein zugänglich sind (§ 28 Abs. 1 Nr. 3 BDSG).[417] Gemäß § 28 Abs. 1 S. 2 BDSG sind bei der Datenerhebung die verfolgten Zwecke konkret festzulegen.[418] Für andere Zwecke dürfen die zweckgerichtet erhobenen Daten nur dann genutzt werden, wenn gemäß § 28 Abs. 2 BDSG die Voraussetzungen von § 28 Abs. 1 Nr. 2 oder Nr. 3 BDSG vorliegen.[419]
§§ 29, 30 BDSG sind hingegen für die Beantwortung der in dieser Arbeit zu behandelnden Fragen nicht einschlägig. Im Blickpunkt dieser Arbeit steht die Datenverarbeitung für eigene Zwecke und nicht die geschäftsmäßige Datenerhebung und Datenspeicherung zum Zwecke der Übermittlung.[420]
Was unter „eigenen Geschäftszwecken“ zu verstehen ist, wird an späterer Stelle noch genau erörtert.[421]

[417] Siehe auch Hoeren in: Roßnagel, Handbuch Datenschutzrecht, 4.6 Rn. 15, der darlegt, dass nach § 28 Abs. 1 Nr. 1 BDSG eine Speicherung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke nur in drei voneinander zu trennenden Alternativen zulässig ist. Siehe Simitis in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 63 mit dem Hinweis, dass § 28 zwar der verantwortlichen Stelle das Recht einräumt, personenbezogene Daten auch ohne Einwilligung der Betroffenen gemäß § 4 BDSG zu verwenden, dass aber der Verzicht auf die Einwilligung nicht bedeutet, die Daten ohne weiteres an ihnen vorbei zu erheben.
[418] Vgl. Däubler, NZA 2001, 874, 876.
[419] Vgl. Däubler, NZA 2001, 874, 877.
[420] Siehe zu § 29 BDSG (geschäftsmäßige Datenerhebung und –speicherung zum Zweck der Übermittlung) sowie zu § 30 BDSG (geschäftsmäßige Erhebung und Speicherung zum Zweck der Übermittlung in anonymisierter Form) etwa Hoeren in: Roßnagel, Handbuch Datenschutzrecht, 4.6 Rn. 56 ff. § 29 BDSG gilt beispielsweise für so genannte Adresshändler, die personenbezogene Daten gewerbsmäßig bearbeiten (vgl. Evers/Kiene, NJW 2726, 2729 Fn.8, dort mit Verweis auf Büllesbach, CR 2000, 544, 548 sowie OLG Hamm, NJW 1996, 131, 131). Zur Anwendbarkeit von § 29 BDSG im Rahmen des Scoring-Verfahrens der SCHUFA siehe Wuermeling, NJW 2002, S. 3508 ff.
[421] Siehe hierzu S. 208 ff., 388 ff.

b. Telekommunikationsgesetz

§§ 91 ff. TKGenthalten gegenüber dem BDSG vorrangige Regelungen bezüglich der Erhebung und Verarbeitung personenbezogener Daten von natürlichen Personen durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken.[422] Gemäß § 91 Abs. 1 TKG stehen außerdem dem Fernmeldegeheimnis[423] unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder Personengesellschaft, sofern sie mit der Fähigkeit ausgestattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, den personenbezogenen Daten gleich. Vom Fernmeldegeheimnis sind hierbei insbesondere Verbindungsdaten eines Kommunikationsvorganges erfasst, d.h. wer, wann, mit wem, wie lange, von wo, wohin und auf welche Weise kommuniziert hat,[424] sowie der Inhalt der Kommunikation.[425]

Das TKG unterscheidet insgesamt zwischen Bestandsdaten gemäß § 3 Nr. 3 TKG sowie Verkehrsdaten gemäß § 3 Nr. 30 TKG.[426]

---

[422] Siehe zum Telekommunikationsgesetz Fn. 28. Die TDSV (in der Fassung vom 18.12.2000), die durch §§ 91 ff. TKG nunmehr ersetzt worden ist (vgl. hierzu Fn. 28), hat im Übrigen die in der Ermächtigungsgrundlage des § 89 Abs. 2 TKG a.F. genannten Erlaubnistatbestände lediglich konkretisiert (vgl. Hanau/Hoeren/Andres, Private Internet-Nutzung durch Arbeitnehmer, S. 43; Hilber/Frik, RdA 2002, 89, 93). Siehe zum Ex

[423] Zum Begriff des Fernmeldegeheimnisses siehe Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 11; Büttgen in: Hoeren/Sieber, Teil 16.3 Rn. 38; Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 113; Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 85 TKG(1998), Band 1, Rn. 11; K. Lau in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 88 TKG(2004), Band 2, Rn. 18 sowie mit dem Hinweis unter Rn. 17, dass sich das Fernmeldegeheimnis ebenso auf Individualkommunikation wie beispielsweise E-Mail erstreckt..

[424] Büchner in: TKG-Kommentar, § 85 TKG Rn. 3; Büllesbach, CR 2000, 11, 15; Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 113.

[425] Geschützt ist das Interesse des Einzelnen, sowohl den Inhalt als auch die näheren Umstände der Telekommunikation geheim zu halten (Büttgen in: Hoeren/Sieber, Teil 16.3 Rn. 38). Siehe auch Klesczewski in: Berliner Kommentar zum TKG, § 88 TKG Rn. 14, der auf die Rechtsprechung des Bundesverfassungsgerichts verweist (BverfGE 67, 157, 172), wonach unter Artikel 10 GG nicht nur der Kommunikationsinhalt fällt, sondern auch die näheren Umstände des Kommunikationsvorgangs (ob und wann zwischen welchen Personen ein Telekommunikationsvorgang stattgefunden hat).

[426] Siehe auch § 2 Nr. 4 TDSV sowie Fn. 28, wo darauf hingewiesen worden ist, dass der Begriff der Verbindungsdaten im novellierten TKG durch den Begriff der Verkehrsdaten ausgetauscht worden ist, damit aber keine inhaltlichen Änderungen verbunden sind.

aa. Verarbeitung von Bestandsdaten

Bestandsdaten sind gemäß § 3 Nr. 3 TKG[427] die Grunddaten des Vertragsverhältnisses.[428] Der Begriff beinhaltet sämtliche personenbezogene Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.

In § 95 TKG ist eine Regelung über die Verarbeitung von Bestandsdaten enthalten, die gemäß § 95 Abs. 1 TKG die Erhebung und Verarbeitung der Bestandsdaten davon abhängig macht, dass diese zur Erreichung des in § 3 Nr. 3 TKG genannten Zwecks, demgemäß zur Begründung, inhaltlichen Ausgestaltung und Änderung eines Vertragsverhältnisses mit einem Teilnehmer, erforderlich ist.[429] Eine Information ist zur Erfüllung einer Aufgabe nur dann erforderlich, wenn die Aufgabe ohne Kenntnis der Information nicht, nicht rechtzeitig, nur mit unverhältnismäßigem Aufwand oder mit sonstigen unverhältnismäßigen Nachteilen erfüllt werden kann.[430]

[427] § 2 Nr. 3 TDSV enthielt eine entsprechende Definition und regelte, dass Bestandsdaten personenbezogene Daten eines an der Telekommunikation Beteiligten sind, die erhoben werden, um ein Vertragsverhältnis über Telekommunikationsdienste einschließlich dessen inhaltlicher Ausgestaltung mit dem Diensteanbieter zu begründen oder zu ändern.
[428] Vgl. auch Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 111; Engel-Flechsig, RDV 1997, 59, 65.
[429] Siehe zur Verarbeitung von Bestandsdaten auch Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 39, der ebenso auf die übrigen Verarbeitungstatbestände eingeht. Nach § 95 Abs. 1 S. 2 TKG ist die Speicherung und Verarbeitung der Bestandsdaten der Teilnehmer von Diensteanbietern durch einen anderen Telekommunikationsdiensteanbieter zulässig ist, soweit dies zur Erfüllung des Vertrages zwischen beiden erforderlich ist. Außerdem darf der Diensteanbieter die Bestandsdaten seiner Teilnehmer und der Teilnehmer seiner Diensteanbieter zur Beratung der Teilnehmer, zur Werbung und zur Marktforschung gemäß § 95 Abs. 2 TKG nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat.
[430] Globig in: Roßnagel, Handbuch Datenschutzrecht, 4.7 Rn. 95. Siehe zur Erforderlichkeit im Arbeitsverhältnis Däubler, NZA 2001, 874, 876. Die „Nützlichkeit" ist nicht ausreichend.

bb. Verarbeitung von Verkehrsdaten

Bei Verkehrsdaten gemäß § 3 Nr. 30 TKG handelt es sich um Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.
§ 96 Abs. 1 TKG enthält eine Aufzählung von Verkehrsdaten, die erhoben und verwendet werden dürfen, soweit dies für die in § 91 bis § 107 TKG genannten Zwecke erforderlich ist.[431] Unter die abschließende Aufzählung[432] fällt die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten, den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen, den vom Nutzer in Anspruch genommenen Telekommunikationsdienst, die Endpunkte von fest geschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen, sowie sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

cc. Verarbeitung von „besonderen Verkehrsdaten“

aaa. Standortdaten

In § 3 Nr. 19 TKG ist erstmals eine eigenständige Definition über Standortdaten zu finden. Danach sind Standortdaten Daten, die in einem Telekommunikationsnetz erhoben, verarbeitet oder genutzt werden und die den geographischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben. Auch Standortdaten sind Verkehrsdaten.[433]

---

[431] Zur Erforderlichkeit siehe die gerade dargestellte Defintion und den Verweis in Fn. 430.
[432] Siehe zur abschließenden Auflistung Büchner in: TKG-Kommentar (2. Auflage), § 5 TDSV (Anh § 89 TKG) Rn. 1; Robert in: TKG-Kommentar (3. Auflage), § 96 TKG Rn. 2 sowie Gramlich in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 89(1998), Band 1, TKG Rn. 45.
[433] Vgl. hierzu Erwägungsgründe 14 und 15 sowie Artikel 6 Abs.1 und Artikel 9 der EU-Richtlinie 2002/58/EG und § 96 Abs. 1 Nr. 1 TKG). Siehe außerdem Schrey/Meister, K&R 2002, 177, 188,

Über die Notwendigkeit einer gewissen Genauigkeit der Angabe des geographischen Standorts bzw. des durch einen gewissen Radius eingrenzbaren exakten Aufenthaltsort ist in § 3 Nr. 19 TKG keine Regelung zu finden. Diesbezüglich enthält die EU-Richtlinie 2002/58/EG keine Vorgaben.[434] Aus § 96 Abs. 1 Nr. 1 TKG ergibt sich jedoch, dass von dem Begriff der Standortdaten zumindest auch die Daten erfasst sind, die bei mobilen Anschlüssen anfallen. Diese Standortdaten können in Bezug auf die Genauigkeit der Lokalisierung des Nutzers erheblich variieren. Denn ein mobiles Endgerät kann beispielsweise GPS (Global Positioning System)[435] verwenden, das satellitengestütze Ortungssystem,[436] welches ein detailliertes Bewegungsprofil ermöglicht.[437]
Es besteht aber ebenfalls die Möglichkeit, von unterwegs das Handy zum Kontaktaufbau mit dem Internet zu verwenden.[438]
Im letzteren Falle ist es vom Netzbetreiber und dessen technischen Möglichkeiten abhängig, wie exakt die Ortung des Nutzers ist.[439] Denn zu bedenken ist, dass die Empfangsstationen der Mobilfunknetzbetreiber auf größere Strecken verteilt stehen können, so dass sich der Nutzer noch weitgehend unbeobachtet bewegen könnte.[440] Mittlerweile ist es jedoch

---

die darauf verweisen, dass Verkehrsdaten den Oberbegriff darstellen, unter den auch Standortdaten fallen.

[434] Siehe Artikel 2 c) der EU-Richtlinie 2002/58/EG, der ebenfalls nur die allgemein gehaltene Definition liefert, dass Standortdaten den geographischen Standort eines Endgeräts angeben.

[435] Nogala/Haverkamp, DuD 2000, 31, 33.

[436] Vgl. Schrey/Meister, K&R 2002, 177, 179.

[437] Siehe Schrey/Meister, K&R 2002, 177, 179. Vgl. außerdem Nogala/Haverkamp, DuD 2000, 31, 33 mit dem Hinweis, dass für militärische Zwecke die präzisen Lokalisierungswerte zwischen ein und bis zehn Meter schwanken, während für zivile Zwecke die Lokalisierungswerte zehn bis hundert Meter betragen. Zu den mobilen Navigationshilfen siehe auch Erwägungsgrund 9 der EU-Richtlinie 2002/58/EG.

[438] Siehe BfD-Info 5, Datenschutz in der Telekommunikation, 2001, S. 69.

[439] Holznagel/Enaux/Nienhaus, Grundzüge des Telekommunikationsrechts, S. 194, die bei der Möglichkeit der Übermittlung der Funkzelle, die sich im Rahmen von Mobiltelefonen ergibt, von einer nicht sehr genauen Überwachungsmöglichkeit ausgehen. Vgl. hierzu ebenso Hellmich, MMR 2002, 152, 152/153.

[440] Es kommt jedoch stets auf die Umstände des Einzelfalls an, denn so verweist auch Fröhle (siehe Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 59) etwa auf die Tochter der British Telecom „BT Cellnet“, die in London allein 800 solcher Basisstationen besitzt und der Handynutzer bis auf 50 Meter genau lokalisiert werden kann. In diesem Fall kann von ständiger Lokalisierung oder auch Überwachungsmöglichkeit gesprochen werden. Siehe auch Nogala/Haverkamp, DuD 2000, 31, 33 mit dem Hinweis, dass die Systemnetze der Mobilfunkbetreiber die weitverbreitesten und zugleich beinah flächendeckenden Raum-Ortungssysteme darstellen. Jedes Handy funktioniere als Sender, das seine Anwesenheit in einer bestimmten Funkzelle einer Sendestation melde. In engmaschigen innerstädtischen Netzen lasse sich so mit dem Verfahren der Aufenthaltsort eines bestimmten Mobilfunkgerätes bis auf wenige Meter genau lokalisieren. Insbesondere die Fortentwicklung UMTS schafft zukünftig die Möglichkeit, den Aufenthaltsort von Telefonkunden bis auf wenige Meter genau zu

technisch ebenso möglich, ein nahezu detailliertes Bewegungsprofil zu erstellen, da Nutzer „bis auf wenige hundert Meter“ lokalisiert werden zu können.[441]
Aber auch für einen Festnetzprovider bestehen Möglichkeiten einer Standortdatenbestimmung.[442]

Da § 3 Nr. 19 TKG sowie Artikel 2 c) der EU-Richtlinie 2002/58/EG nicht zwischen den Standortdaten mobiler Einwahl und Standortdaten von Festnetzverbindungen unterscheidet, gibt es dementsprechend mehrere Arten von Standortdaten. Dabei ist die Begriffsdefinition des § 3 Nr. 19 TKG zunächst „neutral“, so dass die grobe Bestimmbarkeit des Aufenthaltsorts ausreicht,[443] und unabhängig von der Art und Weise des Internetzugangs (mobil oder Festnetz) allein entscheidend ist, dass das Endgerät des Nutzers geografisch zu ermitteln ist.[444] Eine andere Auslegung ist auch nicht der Regelung des § 98 Abs. 1 Nr. 1 TKG zu entnehmen, in welcher lediglich die Zulässigkeit der Verwendung von Standortdaten mobiler Anschlüsse geregelt ist. Diese Regelung war bereits in § 6 Abs. 1 Nr. 1 TDSV enthalten und ist wortgleich übernommen worden, ohne aber zu berücksichtigen, dass sich ein geografischer Standort (wie gerade festgestellt) bei Festnetzverbindungen ermitteln lässt. § 96 Abs. 1 Nr. 1 TKG sollte daher vielmehr so verstanden

---

liefern, siehe hierzu auch Kilian, CR 2002, 921, 921 und Schrey/Meister, K&R 2002, 177, 179, die darauf verweisen, dass die Genauigkeit der Lokalisierung von den örtlichen Gegebenheiten abhängt.

[441] Siehe Schrey/Meister, K&R 2002, 177, 179, die ausführen, dass eine Lokalisierung des Endgeräts im Innenstadtbereich bis auf wenige hundert Meter möglich ist, und VIAG Interkom in manchen Innenstadtbereichen aufgrund der eingesetzten Technik der Funkzellen die Möglichkeit bietet, den Aufenthaltsort in einem Radius zwischen 500 m und 2 km genau zu ermitteln. Vgl. außerdem Kloepfer in: Holznagel/Nelles/Sokol, TKÜV, S. 97 mit dem Hinweis, dass der Aufenthaltsbereich eines Beschuldigten über die Funkzelle, in die er sich mit seinem Handy einwählt, flächendeckend realisierbar und ohne größeren Aufwand möglich ist.

[442] Siehe zu dieser Lokalisierungsmöglichkeit Schrey/Meister, K&R 2002, 177, 178 Fn. 8. Siehe außerdem Welp in: Holznagel/Nelles, Sokol, TKÜV, S. 10 mit dem Hinweis, dass die Verbindungsdaten eines Festnetzanschlusses stets erkennen lassen, dass sich der Benutzer zum Zeitpunkt der Verbindung am Standort des Gerätes aufgehalten hat.

[443] Siehe hierzu auch Schrey/Meister, K&R 2002, 177, 188/189, die ebenfalls davon ausgehen, dass im Sinne der EU-Richtlinie 2002/58/EG zwischen zwei Arten von Standortdaten zu differenzieren ist, und dass für Standortdaten, die die Position des Nutzers genauer angeben, dessen Einwilligung oder die Anonymisierung der Daten notwendig ist. Zur Anonymisierungsmöglichkeit von Standortdaten siehe ebenso Schrey/Meister, K&R 2002, 177, 185/186.

[444] Siehe hierzu insbesondere Schrey/Meister, K&R 2002, 177, 184, die darauf verweisen, dass die eigene Erhebung von Standortdaten eines Festnetzproviders einen erheblichen technischem Aufwand bedeute. Damit ist aber ebenso klar gestellt, dass es grundsätzlich möglich ist.

werden, dass ein Anbieter grundsätzlich „auch“ Standortdaten mobiler Anschlüsse verwenden darf, aber „erst recht“ Standortdaten, die bei Festnetzverbindungen anfallen, da letztere regelmäßig weniger genaue Lokalisierungsmöglichkeiten erlauben. Eine solche Auslegung steht im Einklang mit Artikel 2 c) der EU-Richtlinie 2002/58/EG, welcher nicht zwischen mobilen Anschlüssen und Festnetzanschlüssen unterscheidet. Darüber hinaus wird insbesondere die Fortentwicklung der Technik beachtet, die unter Umständen ebenso bei Festnetzanschlüssen (genauere) Lokalisierungsmöglichkeiten ermöglichen wird.

bbb. Dienst mit Zusatznutzen

In § 98 TKG ist eine eigenständige Regelung bezüglich der Verarbeitung von Standortdaten eingefügt worden.[445]
Nach dieser Regelung dürfen Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten verwendet[446] werden, nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert[447] wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat.
Nach § 3 Nr. 5 TKG ist „Dienst mit Zusatznutzen“ jeder Dienst, der die Erhebung, Verarbeitung oder Nutzung von Verkehrsdaten oder Standortdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Entgeltabrechnung dieses Vorganges erforderliche Maß hinausgeht.[448] Die entsprechende Grundlage dieser Formulierung ist der EU-Richtlinie 2002/58/EG zu entnehmen, wobei in Erwägungsgrund 18 dieser Richtlinie beispielhaft unter anderem Navigationshilfen, Verkehrsinformationen und Wettervorhersage als Dienste mit Zusatznutzen aufgezählt werden.

[445] Zurückzuführen ist diese gesetzliche Regelung auf die EU-Richtlinie 2002/58/EG, in deren Artikel 9 eine nahezu wortgleiche Regelung zu finden ist. In der TDSV war eine entsprechende Regelung noch nicht enthalten. Siehe zu den in der EU-Richtlinie 2002/58/EG geregelten Standortdaten auch Grapentin in: Bräutigam/Leupold, Online-Handel, Kapitel B X Rn. 88 ff.
[446] Die Bedeutung von „Verwenden“ ergibt sich mittelbar aus dem Gesetz, da § 3 Abs. 5 BDSG regelt, dass Nutzen jede Verwendung von Daten bedeutet, soweit es sich nicht um Verarbeitung im Sinne von § 3 Abs. 4 BDSG handelt; siehe auch Gola/Schomerus, BDSG, § 3 BDSG Rn. 41 ff.
[447] Siehe S. 106 zur Definition der Anonymisierung gemäß § 3 Abs. 6 BDSG.
[448] Siehe Erwägungsgrund 18 sowie Artikel 2g) und Artikel 9 der EU-Richtlinie 2002/58/EG bzw. der im TKG erfolgten entsprechenden Umsetzung in § 3 Nr. 5 TKG und § 98 TKG.

Diese Definitionen der EU-Richtlinie 2002/58/EG entsprechen der Regelung in § 2 Abs. 1 TDG, da unter den Begriff des Teledienstes laut Gesetz beispielsweise Telebanking, Telespiele und Datendienste wie Börsen- oder Wetternachrichten fallen.[449]

Daher ist davon auszugehen ist, dass aufgrund der identischen Definitionen und beispielhaften Aufzählungen Teledienste und Dienste mit Zusatznutzen zumindest zum Teil identisch sind. Zu berücksichtigen ist jedoch die von § 2 Abs. 1 TDG abweichende Zielrichtung, die einem Dienst mit Zusatznutzen immanent ist. Denn dieser ist darüber hinaus in einem engeren Sinne zu verstehen. Aus der Formulierung des Artikels 2 g), des Artikels 9 sowie dessen Erwägungsgrund 18 der EU-Richtlinie 2002/58/EG ergibt sich, dass ein Dienst mit Zusatznutzen gerade auf der Erhebung von Standortdaten basieren muss bzw. der Dienst mit Zusatznutzen ohne die Erhebung von Standortdaten gar nicht erbracht werden könnte. Dabei ist nicht relevant, ob nur eine grobe Standortbestimmung erfolgen oder aber ein detailliertes Bewegungsprofil erstellt werden kann. Denn die in Erwägungsgrund 18 der EU-Richtlinie 2002/58/EG beispielhaft genannten Dienste wie Wettervorhersage oder touristische Informationen können sich grundsätzlich ebenso auf größere Gebiete bzw. Territorien erstrecken.[450]

Die Dienste mit Zusatznutzen haben unter Beachtung dieser Erwägungsgründe der EU-Richtlinie 2002/58/EG vielmehr die Gemeinsamkeit, dass die Standortdatenverarbeitung gerade zum Zwecke der Erbringung der Dienstleistung erfolgt oder zumindest wesentlicher Leistungsinhalt ist. Aber auf jeden Fall ist mehr gefordert, als eine Standortdatenverarbeitung allein zum Zweck der Übermittlung einer Nachricht oder für Fakturierungszwecke durchzuführen.[451]

Insgesamt ist ein Dienst mit Zusatznutzen daher teilidentisch mit einem Teledienst, da er stets ein inhaltliches Angebot beinhaltet.

Aber einschränkend muss gelten, dass ein Dienst mit Zusatznutzen allein für inhaltliche Angebote gilt, deren Voraussetzung es gerade ist, Standortdaten für dieses inhaltliche Angebot zu verarbeiten. Dies gilt stets unabhängig davon, ob

[449] Der Begriff der Telekommunikation in § 2 Abs. 1 TDG ist im Übrigen als Verweis auf die Definition des § 3 Nr. 22 TKG zu verstehen (Spindler in: Roßnagel, Recht der Multimedia-Dienste, § 2 TDG Rn. 17).

[450] So ändern sich Wetter- und Touristeninformationen nicht „straßenweise".

[451] Siehe Artikel 2 g) der EU-Richtlinie 2002/58/EG.

auf weitläufige Gebiete bezogen, wie es etwa bei Wetternachrichten oder Tarifberatung der Fall sein kann, oder auf engere Regionen oder gar auf einzelne Städte begrenzt, um beispielsweise Hotel- und Restaurantangebote zu verbreiten.[452]

c. Teledienstedatenschutzgesetz

Das Teledienstedatenschutzgesetz (TDDSG) trennt bezüglich der Verarbeitung von Daten bei Telediensten zwischen Bestands- und Nutzungsdaten[453] und enthält diesbezüglich gegenüber dem BDSG vorrangige Regelungen.

aa. Verarbeitung von Bestandsdaten

Bestandsdaten sind gemäß § 5 TDDSG solche Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit dem Diensteanbieter über die Nutzung von Telediensten erforderlich sind.[454] Für diesen Zweck dürfen Bestandsdaten verarbeitet werden.

bb. Verarbeitung von Nutzungsdaten

§ 6 TDDSG enthält Regelungen bezüglich Nutzungsdaten bzw. Abrechnungsdaten.
Gemäß § 6 Abs. 1 TDDSG darf ein Diensteanbieter Nutzungsdaten, nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen.

---

[452] Bei letzteren wird der Standort also gerade aus dem Grund festgestellt wird, um eine Dienstleistung zu erbringen, die mit den sachlichen Verhältnisses dieses Standorts in unmittelbaren Zusammenhang steht. Schrey/Meister, K&R 2002, 177, 179 führen das Beispiel an, dass der Besitzer eines italienischen Restaurants im Stadtteil Z der Stadt X, allen Nutzern, die sich im Umkreis von 1000 m um sein Restaurant aufhalten, gezielt Pizza-Angebote unterbreiten könnte. Siehe außerdem Ohlenburg, MMR 2004, 431, 436, zur Möglichkeit des Nutzers, sich das nächstgelegene Hotel mitteilen zu lassen. Zur ortsbezogenen Suche nach Geldautomaten, Restaurants, Cafés und Tankstellen siehe Hellmich, MMR 2002, 152, 152.

[453] Zum Teledienstedatenschutzgesetz siehe S. 7. Der MDStV enthält in §§ 12 ff. dem TDDSG vergleichbare Datenschutzbestimmungen (siehe zum MDStV Fn. 33) und wird in dieser Arbeit daher nicht gesondert behandelt (vgl. zu den identischen Voraussetzungen des TDDSG und des MDStV auch Büchner in: TKG-Kommentar (2. Auflage), § 89 TKG Rn. 13).

[454] Siehe Bäumler, DuD 1999, 258, 261, der ausführt, dass der Begriff der Bestandsdaten mit dem gleichen Begriff aus dem Telekommunikationsrecht verwandt ist und die für die Abwicklung eines Teledienste-Vertrages notwendigen (Grund-)Daten betrifft. Zur Erforderlichkeit siehe S. 98.

§ 6 Abs. 4 TDDSG regelt insoweit ergänzend, dass dem Diensteanbieter nur gestattet ist, Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus zu verarbeiten und zu nutzen, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind.[455]

Das TDDSG enthält allerdings keine dem § 88 TKG entsprechende Regelung bezüglich des Fernmeldegeheimnisses und des Inhalts der Kommunikation. So gibt es aber ebenso bei der Nutzung eines Teledienstes personenbezogene Daten, die als Kommunikationsinhalt geschützt werden müssen. Dies kommt beispielsweise beim Ausfüllen eines Webformulars in Betracht. Solche Datenwerden als Inhaltsdaten bezeichnet, wobei der Begriff der Inhaltsdaten gesetzlich nicht definiert ist.[456] Die Anwendbarkeit von TDDSG oder BDSG ist hierbei umstritten, wobei nach überwiegender Meinung der Inhalt der Kommunikation bei einem Teledienst jedoch gemäß den Regelungen des BDSG geschützt sein soll.[457]

---

[455] Dix/Schaar in: Roßnagel, Recht der Multimedia-Dienste, § 6 TDDSG Rn. 149 ff.

[456] Vgl. Geis, Recht im eCommerce, S. 140, der an dieser Stelle ebenfalls darauf verweist, dass Artikel 10 Abs. 5 BTX-Staatsvertrag keine Sonderregelung für Inhaltsdaten enthält; vgl. hierzu auch Imhof, CR 2000, 110, 113; Geis, RDV 2000, 208, 209.

[457] Siehe Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 110; Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2987 Fn. 52; Schaar, Datenschutz im Internet, Rn. 450, 465; Gola/Klug, Grundzüge des Datenschutzrechts, S. 191; Scholz in: Roßnagel, Datenschutz beim Online-Einkauf, S. 44; Schrey/Meister, K&R 2002, 177, 181; Bäumler, DuD 1999, 258, 259; Gola/Müthlein, RDV 1997, 192, 196; Schaar, CR 1996, 170, 172/173 (für die Anwendbarkeit des BDSG). Vgl. auch Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDDSG Rn. 59/61, der anmerkt, dass das TDDSG zwar gegenüber dem BDSG die spezielleren Regelungen enthält, aber soweit personenbezogene Daten Inhalte des Angebots oder der Nutzung darstellen, ihre Erhebung und Verarbeitung den allgemeinen Datenschutzregelungen unterliegt (z.B. Inhaltsdaten eines Webformulars), sowie Dix in: Roßnagel, Recht der Multimedia-Dienste, § 5 TDDSG Rn. 54, der danach unterteilt, dass nur die Daten, die durch die Nutzung des Teledienstes angefallen sind (wie beispielsweise Angaben über Hard- und Software) dem TDDSG unterliegen sollen, während bezüglich der Kundendaten das allgemeine Datenschutzrecht Anwendung finden soll. Vgl. außerdem Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 96/97, 148 ff., der eine subsidiäre Anwendung des BDSG in Betracht zieht, soweit Inhaltsdaten verarbeitet werden. Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDDSG Rn. 61 weist allerdings darauf hin, dass von einer subsidiären Anwendung nicht gesprochen werden kann, weil hier die beiden Regelungen nebeneinander stehen. A.A (für die Anwendbarkeit des TDDSG) aber: Koenig/Röder, CR 2000, 668, 670/672; Imhof, CR 2000, 110, 113/114/115; Bock, Bräutigam/Leupold, B VII Rn. 135; Geis, Recht im eCommerce, S. 140/141.

3. Pflichten eines Diensteanbieters

Im Folgenden wird ein Prüfungsschema bezüglich der Pflichten eines Diensteanbieters dargestellt, welches im dritten Abschnitt dieser Arbeit „Dienste im VPN und Datenschutz“ zur Anwendung kommen soll.
Im Einzelnen handelt es sich um Fragen der Datenvermeidung, datenschutzrechtliche Unterrichtungspflichten sowie die Sicherstellung von technischen Schutzmaßnahmen. Einen weiteren Prüfungspunkt stellen darüber hinaus die Schranken des Datenschutzes aufgrund staatlicher Auskunfts- und Überwachungspflichten dar.

a. Datenvermeidung

Das Optimum der Datenvermeidung ist erreicht, wenn keine personenbezogenen Daten gemäß § 3 Abs. 3 BDSG erhoben werden, weil in diesem Falle auch keine personenbezogenen Daten gemäß § 3 Abs. 4 BDSG verarbeitet und gemäß § 3 Abs. 5 BDSG genutzt werden können.[458]

Ist Datenentstehung nicht vermeidbar, ist bereits bei der Datenerhebung von den Möglichkeiten der Anonymisierung gemäß § 3 Abs. 6 BDSG und Pseudonymisierung gemäß § 3 Abs. 6a BDSG Gebrauch zu machen ist, soweit dies möglich ist, und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.[459] Anonymisieren bedeutet gemäß § 3 Abs. 6 BDSG das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlich Person zugeordnet werden können. Beim Pseudonymisieren gemäß § 3 Abs. 6a BDSG handelt es sich hingegen um das Ersetzen eines Namens und anderer

[458] Vgl. Bizer in: Simitis, BDSG-Kommentar, § 3a BDSG Rn. 57; Abel, Praxishandbuch Datenschutz, Teil 8/4.3.1 S. 1.
[459] Siehe zum Systemdatenschutz Gola/Schomerus, BDSG, § 3a BDSG Rn. 4/8. Auch die EU-Richtlinie 2002/58/EG beinhaltet als Grundprinzip die Datenvermeidung und Datensparsamkeit, wie sich aus Erwägungsgrund 20 (in welcher der Diensteanbieter zur Aufklärung über Verschlüsselungstechniken verpflichtet wird), Erwägungsgrund 26 (wo auf die Erlaubnis zur Speicherung lediglich für einen begrenzten Zeitraum abgestellt wird) oder Erwägungsgrund 30 (der ausdrücklich die Pflicht normiert, die Systeme derart einzurichten, dass so wenig wie möglich personenbezogene Daten entstehen) ergibt.

Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.[460]
Diese Vorgabe ist in dem Grundsatz des so genannten Systemdatenschutzes gemäß § 3a BDSG enthalten, der als übergreifende Regelung für sämtliche Bereiche des Datenschutzrechts übernommen worden ist. [461]

Allerdings ist zu berücksichtigen, dass nur die Anonymisierung gemäß § 3 Abs. 6 1. Alt. BDSG den Personenbezug durch irreversible Löschung dauerhaft und vollständig beseitigen kann. Die Anonymisierung im Sinne des § 3 Abs. 6 2. Alt BDSG und die Pseudonymisierung gemäß § 3 Abs. 6a BDSG können dies nicht sicherstellen, ,[462] da die Beseitigung des Personenbezugs allein der Löschung als Unkenntlichmachen bzw. Vernichten gespeicherter personenbezogener Daten vorbehalten ist.[463] Die Bestimmbarkeit einer Person und Personenbezogenheit bleibt daher grundsätzlich weiterhin bestehen, auch wenn hierzu ein unverhältnismäßig hoher Aufwand erforderlich ist.[464]
Die Anonymisierung, die gemäß § 3 Abs. 6 2. Alt. BDSG die Herstellung des Personenbezugs erschwert, und die Pseudonymisierung gemäß § 3 Abs. 6a BDSG, die ausschließlich auf das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen beschränkt ist,[465] stellen daher lediglich Instrumente dar, bei der Erhebung und bei unvermeidbarer und länger

[460] Vgl. zur Pseudonymisierung auch Bizer in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 212 ff.
[461] Siehe Rasmussen, CR 2002, 36, 38 sowie die Ausführungen in der Einführung S. 16.
[462] Vgl. Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn.196, der darauf verweist, dass die Qualität der Einzelangaben als personenbezogene Daten bei einer Anonymisierung, die die Voraussetzungen des § 3 Abs.6 2. Alt. BDSG erfüllt, erhalten bleibt.
[463] Siehe die Fn. 58 und den darin enthaltenen Verweis auf Enzmann/Scholz in: Roßnagel, Datenschutz beim Online-Einkauf, S. 84, die vorrangig die Frage nach der Notwendigkeit einer Datenverarbeitung stellen und anschließend auf das Optimum des Datenschutzes durch Bildung anonymer oder pseudonymer Datensätze verweisen. Anonymisierung sollte allerdings durch die Löschung des Personenbezugs erfolgen, da insbesondere auch die Anonymisierung im Sinne von § 3 Abs. 6 1. Alt. BDSG nicht geeignet ist, den Personenbezug dauerhaft auszuschließen (vgl. Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 196). Grundsätzlich ist hierbei zu beachten, dass ebenso die Löschung gemäß § 3 Abs. 4 Nr. 5 BDSG eine Form der Verarbeitung darstellt, so dass sich die Fragestellung nach der Erforderlichkeit der Datenverarbeitung (um es exakter zu formulieren) darauf bezieht, ob es erforderlich ist, dass Daten (längerfristig) entstehen, erfasst oder gespeichert werden. Siehe auch Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 175 zur Löschung als eine irreversible Handlung, die bewirkt, dass eine Information nicht länger aus gespeicherten Daten gewonnen werden kann. Außerdem Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2 Rn. 81 ff.; Gola/Schomerus, BDSG, § 3 BDSG Rn. 40; Schaffland/Wiltfang, BDSG, § 3 BDSG Rn. 75.
[464] Vgl. Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 196.
[465] Vgl. Bizer in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 212 ff.. Siehe zu pseudonymen Daten auch Tinnefeld in: Roßnagel, Handbuch Datenschutzrecht, 4.1 Rn. 30, die auf die Bedeutung „falscher Name“ oder „Deckname“ verweist.

andauernder Speicherung von personenbezogenen Daten, diese Daten „datenschutzfreundlicher“ zu speichern und aufzubewahren.

Dies bedeutet, dass im Sinne eines bestmöglich verwirklichten Datenschutzes stets die Löschung von Daten, die zur Erfüllung legitimer Geschäftszwecke nicht erforderlich sind, [466] das oberste Gebot darstellen muss. Erfolgt keine vollständige und unwiderrufliche Löschung der Daten,[467] kann niemals absolut ausgeschlossen werden, dass der Personenbezug nicht nachträglich hergestellt wird, beispielsweise etwa durch Preisgabe der Daten.[468] Hierbei sind unter anderem die vielfältigen Verknüpfungsmöglichkeiten im Internet zu berücksichtigen.[469] In diesem Zusammen wird stets die mögliche Irreversibilität der einmal gespeicherten Daten betont[470] und darüber hinaus darauf verwiesen, dass dem Nutzer oft verborgen bleibt, wer Daten über ihn sammelt.[471]
Trotz dieser potenziellen Gefahren für das Persönlichkeitsrecht hat der Gesetzgeber allerdings die Anonymisierung von Daten im Sinne von § 3 Abs. 6 2. Alt. BDSG für jedwedes Interesse eines Datenverarbeiters (und als unternehmensfreundliche Alternative) zugelassen.[472]

[466] Vgl. zum Erforderlichkeitsprinzip Roßnagel in: Roßnagel, Handbuch Datenschutzrecht, 1 Rn. 40. Siehe außerdem Bizer in: Simitis, BDSG-Kommentar, § 3a BDSG Rn. 53. Zur Erforderlichkeit siehe außerdem S. 98, wonach eine Information ist zur Erfüllung einer Aufgabe nur dann erforderlich ist, wenn die Aufgabe ohne Kenntnis der Information nicht, nicht rechtzeitig, nur mit unverhältnismäßigem Aufwand oder mit sonstigen unverhältnismäßigen Nachteilen erfüllt werden kann.
[467] Siehe insbesondere Heibey in: Roßnagel Handbuch Datenschutzrecht, 4.5 Rn. 23 zum datenschutzgerechten Löschen und Unkenntlichmachen von Daten im Sinne des § 3 Abs. 3 Nr. 5 BDSG, so dass diese nicht mehr mit handelsüblichen Programmen wiederhergestellt werden können. Heibey (aaO) verweist hierbei auf spezielle Löschungsverfahren, die zu löschende Daten überschreiben oder magnetisieren. Vgl. ebenso Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 200, der ausführt, dass eine Anonymisierung nur bei einer absolut irreversiblen Maßnahme vorliegt. Daher muss auch eine Löschung so durchgeführt werden, dass die Daten tatsächlich nicht mehr zurückgewonnen werden können.
[468] Vgl. hierzu auch Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 35, der sich beispielhaft auf die Übermittlung verschlüsselter Daten an einen Empfänger bezieht und insoweit ausführt, dass diese Daten für den Empfänger anonym sind, aber diese vorher relativ anonymen Daten auch für den Empfänger bestimmbar und damit personenbezogen werden, wenn der Code nachträglich preisgegeben wird. Siehe auch Tinnefeld in: Roßnagel, Handbuch Datenschutzrecht, 4.1 Rn. 23 mit dem Hinweis, dass das Risiko der Re-Individualisierung nie ganz ausgeschlossen werden kann. Ebenso Roßnagel/Scholz, MMR 2000, 721, 726.
[469] Siehe zu den Verknüpfungsmöglichkeiten, der wachsenden Gefahr der Identitätsaufdeckung und den Zusammenführungsmöglichkeiten im Internet Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 51/52; Schaar, Datenschutz im Internet, Rn. 174.
[470] Vgl. etwa Hornung, MMR 2004, 3, 4/5.
[471] De Terwangne/Louveaux, MMR 1998, 451, 451.
[472] Eine Einschränkung ergibt sich lediglich in § 98 TKG.

Im Rahmen dieser Arbeit soll jedoch der Grundsatz der bestmöglichen Datenvermeidung gemäß § 3a BDSG durch eine **vollständige Anonymisierung** im Wege der irreversiblen Datenlöschung im Vordergrund stehen. Mit irreversibler Datenlöschung ist in diesem Zusammenhang die Löschung von Identifikationsmerkmalen, wie beispielsweise Name, Anschrift oder Personenkennungen gemeint. [473] Dies gilt, auch wenn im Einzelfall die Wahrscheinlichkeit zunächst dagegen sprechen sollte,[474] dass eine am Kommunikationsvorgang im Internet beteiligte Person, irgendein Interesse an der Herstellung des Personenbezugs haben könnte, oder ihr das Zusatzwissen zur Herstellung des Personenbezugs fehlt.[475]

Für die Prüfung einer „wirksamen" Datenvermeidung werden daher folgende Fragestellungen im Fokus der Betrachtung stehen:
- Ist die Entstehung von Daten (auf technischen Systemen) erforderlich?[476]
- Und wenn ja, wann können die Daten (auf technischen Systemen) spätestens irreversibel gelöscht werden? [477]

Dies bedeutet, dass ebenso ein Löschungsgebot in Betracht kommen kann, sofern bei einer datenverarbeitenden Stelle Daten (faktisch) anonymisiert entstehen.[478]

Diese Sichtweise empfiehlt sich ebenso aus dem Grunde, da auf diese Weise der Überschaubarkeit der Datenverarbeitung ausreichend Rechnung getragen werden kann. Eine sofortige Löschung nicht erforderlicher Daten bedeutet zudem einen geringeren Aufwand, als wenn die speichernde Stelle fortwährend Prüfroutinen im Sinne des § 3a BDSG vornehmen müsste, um zu überprüfen,

---

[473] Vgl. Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 204/206.
[474] Siehe auch Tinnefeld in: Roßnagel, Handbuch Datenschutzrecht, 4.1 Rn. 23, die darlegt, dass die Personenbeziehbarkeit eine Frage der Wahrscheinlichkeit ist.
[475] Siehe zum Zusatzwissen Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 33.
[476] Zur Erforderlichkeit siehe S. 98.
[477] Vgl. auch Roßnagel in: Roßnagel, Handbuch Datenschutzrecht, 1 Rn. 40, der von einer Verpflichtung zur frühestmöglichen Löschung von personenbezogenen Daten ausgeht.
[478] Siehe zur faktischen Anonymität Tinnefeld in: Roßnagel, Handbuch Datenschutzrecht, 4.1 Rn. 24. Siehe hierzu auch Roßnagel/Scholz, MMR 2000, 721, 726, die darauf verweisen, dass ein gewisses Restrisiko der Aufdeckung nicht zu vermeiden ist und es daher eine Unterscheidung zwischen „absolut anonym" und „faktisch anonym" nicht geben sollte.

ob die (faktische) Anonymität weiterhin besteht.[479] Darüber hinaus kann im Einzelfall die Beurteilung schwierig sein, inwieweit eine Bestimmbarkeit der Person gemäß § 3 Abs. 1 BDSG vorliegt.
Bei der Frage der Bestimmbarkeit muss festgestellt werden, ob die Identität, nötigenfalls unter Verwendung von zugänglichem Zusatzwissen, mit Unterstützung mathematisch-statistischer Experten und unter Rückgriff auf externe Datenverarbeitungs-Kapazität,[480] festgestellt werden kann.

b. Technische Schutzmaßnahmen

Für die Anbieter von Telekommunikationsdiensten ergeben sich außerdem besondere Pflichten, die sich auf die Beachtung und Durchführung von technischen Vorkehrungen beziehen. Daher ist in den einzelnen Personenverhältnissen ebenso die Untersuchung von technischen Schutzmaßnahmen relevant, die im Folgenden dargestellt werden.

aa. Unterrichtungspflichten über Netzsicherheit

Zu den technischen Schutzmaßnahmen können ebenso Unterrichtungspflichten über die Netzsicherheit zählen, wobei zunächst eine Abgrenzung zu den allgemeinen Unterrichtungspflichten des Datenschutzrechts dargestellt wird. Letztere finden sich sowohl im TKG und TDDSG als auch im BDSG.

aaa. Abgrenzung zu allgemeinen Unterrichtungspflichten

Gemäß § 93 S. 2 TKG muss der Diensteanbieter Teilnehmer[481] auf die zulässigen Wahl- und Gestaltungsmöglichkeiten bei der Verarbeitung hinweisen, wobei dies nach § 93 S. 1 TKG bei Vertragsabschluss in einer allgemein verständlichen Form ausreichend ist.[482] Gemäß § 93 S. 3 TKG ist verlangt, dass der Nutzer durch allgemein zugängliche Informationen über die

[479] Vgl. Bizer in: Simitis, BDSG-Kommentar, § 3a BDSG Rn. 54, der auf wiederkehrende Prüf- und Löschungsroutinen Bezug nimmt.
[480] Vgl. Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 33 ff.
[481] Zum Begriff des Teilnehmers siehe S. 8 Fn. 28.
[482] § 93 TKG entspricht weitgehend § 3 Abs. 4 TDSV. Siehe hierzu auch Büchner in: TKG-Kommentar (2. Auflage), § 3 TDSV (Anh § 89 TKG) Rn. 4. Siehe außerdem Büttgen in: TKG-Kommentar (3. Auflage), § 93 TKG Rn1.

Erhebung und Verwendung personenbezogener Daten unterrichtet werden muss.

Sofern die Anwendbarkeit des TDDSG in Frage kommt, muss die gemäß § 3 Abs. 5 TDDSG vorzunehmende Unterrichtung des Nutzers über die Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten darüber hinaus jederzeit abrufbar sein und protokolliert werden.

Unterrichtungspflichten ergeben sich außerdem (sofern nicht vorrangig TKG oder TDDSG Anwendung finden)[483] aus dem BDSG. So regeln §§ 4 Abs. 3, 33 BDSG die Unterrichtung des Betroffenen, wenn personenbezogene Daten erhoben werden.[484]
Diese letztgenannten Unterrichtungspflichten des BDSG sind insbesondere unabhängig von jedweder Diensterbringung zu sehen, sondern richten sich grundsätzlich an Datenverarbeiter, die personenbezogene Daten von Betroffenen verwenden.

bbb. Aufklärungspflicht über Verschlüsselungen

Über diese allgemeinen Unterrichtungspflichten hinaus gelten für Diensteanbieter im Sinne von § 3 Nr. 6 TKG besondere Unterrichtungspflichten über die Netzsicherheit.
In dieser Arbeit wird die Auffassung vertreten, dass eine solche Verpflichtung unmittelbar aus den Regelungen des Artikel 4 der EU-Richtlinie 2002/58/EG sowie § 109 TKG hergeleitet werden kann, was wie folgt begründet wird:

Aus Artikel 4 der EU-Richtlinie 2002/58/EG ergibt sich die Pflicht des Anbieters eines Telekommunikationsdienstes, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit seiner Dienste zu gewährleisten. Eine entsprechende Umsetzung von Artikel 4 der EU-Richtlinie 2002/58/EG kann § 109 TKG entnommen werden. Gemäß § 109 Abs. 1 TKG haben

[483] Siehe zum Exklusivitätsverhältnis S. 92.
[484] Siehe auch Gola/Schomerus, BDSG, § 33 BDSG Rn. 7, mit dem Hinweis, dass von der Benachrichtigungspflicht nach § 33 BDSG vorgelagerte Informationspflichten zu unterscheiden sind, deren Erfüllung die nochmalige Benachrichtigungspflicht entfallen lässt.

nunmehr *alle* Diensteanbieter, die geschäftsmäßig[485] Telekommunikationsdienste erbringen, Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogenen Daten sowie zur Abwehr von unerlaubten Zugriffen auf Daten- bzw. Telekommunikationsverarbeitungssystemen zu treffen. Hierzu kann ebenso die Pflicht des Anbieters eines Telekommunikationsdienstes zur Verschlüsselung der Daten gehören.[486]

Sofern der Diensteanbieter diesen Schutz nicht selbst sicherstellen kann und ihm eine Verschlüsselung nicht selbst möglich ist, hat er nach der Intention des Artikel 4 Abs. 2 der EU-Richtlinie 2002/58/EG als angemessene Schutzmaßnahme zumindest die Verpflichtung, über mögliche Abhilfen zu unterrichten, wenn ein besonderes Risiko der Verletzung der Netzsicherheit besteht.[487]

Diese Auffassung wird im Übrigen durch Erwägungsgrund 20 der EU-Richtlinie 2002/58/EG gestützt und bestätigt. Hierin ist die Regelung enthalten, dass die Diensteanbieter die Nutzer und Teilnehmer über Maßnahmen zum Schutz ihrer zu übertragenden Nachrichten informieren sollen, wie z. B. den Einsatz spezieller Software oder von Verschlüsselungstechniken. Es wird zudem ebenso klargestellt, dass die Anforderung, die Teilnehmer über besondere Sicherheitsrisiken aufzuklären, einen Diensteanbieter nicht von der Verpflichtung entbindet, auf eigene Kosten unverzüglich geeignete Maßnahmen zu treffen, um einem weiteren, unvorhergesehenen Sicherheitsrisiko vorzubeugen

und den normalen Sicherheitsstandard des Dienstes wiederherzustellen.

Eine wortgleiche Regelung im Sinne des Erwägungsgrundes 20 der EU-Richtlinie 2002/58/EG ist zwar im TKG nicht zu finden.[488] Jedoch normiert

---

[485] Zur Geschäftsmäßigkeit siehe S. 83.

[486] Siehe hierzu auch die Ausführungen von Koenig/Röder, CR 2000, 668 ff. bezüglich der EG-Datenschutzrichtlinie, welche wie oben dargestellt (S. 8 Fn. 29), von der EU-Richtlinie 2002/58/EG abgelöst worden ist. Die Verfasser gehen davon aus (aaO 671/672), dass im Sinne der Richtlinie jeder Diensteanbieter geeignete technische und organisatorische Maßnahmen ergreifen muss, um die Sicherheit seiner Dienste zu gewährleisten, insoweit die Netzsicherheit davon betroffen ist.

[487] Vgl. auch Gola/Klug, Grundzüge des Datenschutzrechts, S. 199.

[488] § 3 Abs. 5 TDSV 1996 enthielt noch die Verpflichtung des Diensteanbieters, die Beteiligten in angemessener Weise über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Hierbei wird die Auffassung vertreten, dass diese Regelung durch § 6 Abs. 3 i.V.m. Abs. 2 Nr. 1 TKV erfasst ist (Büchner in: TKG-Kommentar (2. Auflage), § 4 TDSV

§ 93 TKG, wie gerade dargestellt, die Verpflichtung des Anbieters eines Telekommunikationsdienstes, die Teilnehmer über die Verwendung personenbezogener Daten so zu unterrichten, so dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Da damit ebenso die Herstellung von Transparenz über das Wie der Datenverarbeitung verbunden ist,[489] gehört zu den Grundlagen der Datenverarbeitung dementsprechend gemäß der Intention der EU-Richtlinie 2002/58/EG die Sicherstellung der Sicherheit des Dienstes durch besondere Unterrichtungspflichten.

Insoweit besteht zwar eine Überschneidung zu den Pflichten nach § 93 TKG.. Da jedoch die Unterrichtungspflicht bezüglich der Netzsicherheit nach der hier vertretenen Auffassung über die Pflichten des § 93 TKG hinausgeht und diese konkretisiert, wird diesbezüglich ein eigener datenschutzrechtlicher Prüfungspunkt unter dem Oberbegriff „Technische Schutzmaßnahmen" festgelegt.

bb. Anforderungen an technische Systeme

Wie gerade festgestellt ist der Diensteanbieter gemäß § 109 Abs. 1 TKG zur Sicherstellung der angemessenen Maßnahmen zum Schutze des Fernmeldegeheimnisses und der personenbezogenen Daten sowie der Datenverarbeitungssysteme gegen unerlaubte Zugriffe verpflichtet, soweit ihm dies möglich ist.[490]

Nunmehr sind die Schutzziele „Fernmeldegeheimnis und Datenschutz" von jedem zu beachten, der Telekommunikationsdienste erbringt. Eine rechtliche

---

(Anh § 89 TKG) Rn. 4). Zu berücksichtigen ist jedoch, dass vom TKV lediglich Telekommunikationsdienstleistungen für die Öffentlichkeit umfasst sind, während das TKG und die EU-Richtlinie 2002/58/EG für jedwede Telekommunikationsdienstleistung Anwendung findet (zur TKV siehe Fn. 49).

[489] Vgl. Büchner in: TKG-Kommentar (2. Auflage), § 3 TDSV (Anh § 89 TKG) Rn. 4.

[490] Vgl. auch Ehmer in: TKG-Kommentar (2. Auflage), § 87 TKG Rn. 18, der darauf verweist, dass die Verpflichtung nur insoweit besteht, wie die Verantwortlichkeit und unmittelbare Einflussmöglichkeit des Anbieters reicht. Siehe aber zur Verantwortung der Betreiber bei gemeinsamer Nutzung von Standorten Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 39.

Regelung zur Umsetzung dieser Schutzziele durch technische und organisatorische Maßnahmen gab es bislang nur in § 9 BDSG.[491]

Die Maßnahmen zum Schutz der Infrastruktur, z.B. vor Störungen, äußeren Angriffen und Katastrophen, obliegen nur noch Betreibern öffentlicher Telekommunikationsanlagen[492] gemäß §§ 109 Abs. 2, Abs. 3 TKG. Unter den Begriff der Telekommunikationsanlagen als „technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren" fallen auch Server oder Router zur Steuerung und Vermittlung von Online-Kommunikation.[493] Nach § 109 Abs. 2 TKG hat derjenige, der Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, darüber hinaus bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und zum Schutze von Telekommunikations- und Datenverarbeitungssystemen gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen.[494]

Auch wenn diese Maßnahmen in erster Linie der öffentlichen Sicherheit dienen, sollen diese in dieser Arbeit dennoch unter dem datenschutzrechtlichen Gesichtspunkt ergänzend behandelt werden, da der zwischen dem Betreiber einer öffentlichen Telekommunikationsanlage und einem Nutzer oder Teilnehmer zu gewährleistende Datenschutz zumindest mittelbar beeinflusst wird. Denn beispielsweise ist der Betreiber einer öffentlichen Telekommunikationsanlage gemäß § 109 Abs. 3 Nr. 3 TKG zur Erstellung eines überzeugenden Sicherheitskonzeptes verpflichtet, aus dem hervorgeht, welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der

[491] Siehe Begründung zum TKG-E, S. 124. Zur Spezialvorschrift des § 109 TKG gegenüber § 9 BDSG siehe Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 10.
[492] Der Begriff der Telekommunikationsanlage, der den Begriff der Fernmeldeanlage ersetzt hat, ist weit auszulegen (vgl. auch Krader, Das neue Telekommunikationsrecht in der Praxis, S. 117, die auf die Offenheit des Begriffs für technische Entwicklungen verweist und ebenso auf Server und Router im Internet als Telekommunikationsanlagen Bezug nimmt.
[493] Vgl. Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 2; Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 11; Wuermeling/Felixberger, CR 1997, 230, 233; Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 85 TKG(1998), Band 1, Rn. 11;.
[494] Siehe hierzu außerdem Zimmer, CR 2003, 893, 896.

Verpflichtungen aus § 109 Abs. 1 TKG getroffen oder geplant sind. Der Betreiber einer Telekommunikationsanlage muss zunächst beurteilen, welche Gefährdungen seinen Dienst bedrohen und welche technischen Vorkehrungen er dagegen treffen kann,[495] wobei er gleichfalls organisatorische Regelungen für ein effizientes Krisenmanagement treffen sollte.[496] Er muss insbesondere darauf achten, dass die Beschreibung der technischen Vorkehrungen so detailliert sein ist, dass die Bundesnetzagentur diese nachvollziehen kann.[497]

Diese Pflichten sind nicht nur für die öffentliche Sicherheit relevant, sondern haben ebenso Auswirkung darauf, dass Datenschutz im Verhältnis zu einem Teilnehmer und Nutzer in besonderem Maße beachtet und sichergestellt wird, so dass ein zusätzlicher Schutzfaktor für den Teilnehmer und Nutzer besteht. Damit ist zur Abgrenzung der Pflichten in einem VPN von Bedeutung, ob und wer als Betreiber einer öffentlichen Telekommunikationsanlage gemäß § 109 Abs. 2 TKG in Betracht kommt.[498]
Diese Regelung beinhaltet im Übrigen eine Verschärfung zu § 87 Abs. 2 TKG a.F., da nun nicht mehr an das Überschreiten von Grundstücksgrenzen angeknüpft wird.[499]

Im Rahmen des TDDSG ist als Schutzmaßnahme, welcher man technischen Charakter zusprechen kann, lediglich die Regelung des § 4 Abs. 2 Nr. 4 TDDSG zu nennen, die als Vorgabe enthält, dass personenbezogene[500] Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden können.

---

[495] Vgl. Zimmer, CR 2003, 893, 897/898.
[496] Vgl. ebenso Zimmer aaO, die ebenso auf die Hinweise im IT-Grundschutzhandbuch (bzw. nunmehr IT-Grundschutz-Kataloge), Sicherheit in der Informationstechnik, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik, Loseblattsammlung, Stand 2005, abrufbar unter www.bsi.de verweist.
[497] Vgl. Zimmer aaO.
[498] Siehe Zimmer, CR 2003, 893, 896, die einerseits klarstellt, dass im Hinblick auf § 109 Abs. 2 TKG geschlossene Benutzergruppen privilegiert sind, aber andererseits darauf verweist (vgl. Zimmer, CR 2003, 893, 896 Fn. 5), dass auch geschlossene Benutzergruppen in den Anwendungsbereich des
§ 109 Abs. 1 TKG fallen.
[499] Vgl. Zimmer, CR 2003, 893, 897. Zur Abschaffung der Lizenzpflicht gemäß § 6 TKG a.F. siehe Fn. 93.
[500] Der Begriff der personenbezogenen Daten wird auf S. 92 ff. näher definiert und meint gemäß § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Im Hinblick auf die Datenverarbeitung gemäß der Regelungen des BDSG enthält § 9 BDSG die Regelung, dass die datenverarbeitenden Stellen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen haben, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. Hierbei ist das Verhältnismäßigkeitsprinzip zu beachten.[501]

4. Schranken durch gesetzliche Überwachungs- und Auskunftspflichten

Zu einer vollständigen datenschutzrechtlichen Prüfung gehört ebenso die Frage, inwieweit etwaige Einschränkungen aufgrund staatlicher Auskunfts- und Überwachungspflichten innerhalb eines VPN in Betracht kommen können. Daher soll im Folgenden auf die Pflichten eines Diensteanbieter gemäß § 3 Telekommunikations-Überwachungsverordnung (TKÜV)[502] sowie § 113 TKG eingegangen werden.

Gemäß § 3 TKÜV muss der Anbieter, der Telekommunikationsdienste für die Öffentlichkeit anbietet, den berechtigten Stellen Überwachungsmaßnahmen ermöglichen und gegebenenfalls den Inhalt der Kommunikation bereitstellen.[503] Berechtigte Stellen sind im Sinne von § 3, 2 Nr. 3 TKÜV Richter, Staatsanwälte und die in ihrem Polizeidienst tätigen Ermittlungspersonen (§ 100 b Abs. 3 StPO), das Zollkriminalamt sowie die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst (§ 1 Abs. 1 Nr. 1 des Artikel 10-Gesetzes).[504]
§ 3 TKÜV nimmt darüber hinaus auf den Begriff des „Telekommunikationsdienstes für die Öffentlichkeit“ Bezug, also auf einen Dienst, der für die Allgemeinheit erbracht wird.

---

[501] Siehe Gola/Schomerus, BDSG, § 9 BDSG Rn. 5; siehe außerdem Schaffland/Wiltfang, BDSG, § 9 BDSG Rn. 5, die darauf verweisen, dass durch diesen Grundsatz sichergestellt wird, dass der Gesetzgeber nicht übertriebene Forderungen stellt.
[502] Zur TKÜV siehe die Ausführungen in der Einführung S. 12.
[503] Siehe auch Ullrich in: Holznagel/Nelles/Sokol, TKÜV, S. 15 und der Ausführung, dass die Verordnung selbst die Überwachung der Telekommunikation nicht vorsieht, sondern dies in den entsprechenden Rechtsgrundlagen der StPO, im Zollfahndungsdienstegesetz und im G-10-Gesetz vorbehalten sein. Dies sind die Gesetze aufgrund der das in Artikel 10 GG verankerte Post- und Fernmeldegeheimnis eingeschränkt werden darf, wobei für die Polizei dies §§ 100a und 100b Abs. 3 StPO, für das Zollkriminalamt die § 23a Abs. 1 S. 1 des Zollfahndungsdienstegesetzes und für die Sicherheitsbehörden das Gesetz zur Beschränkung des Artikels 10 GG (G-10-Gesetz) sind (siehe auch Zwingel in: Holznagel/Nelles/Sokol, TKÜV, S. 38).
[504] Vgl. Zwingel in: Holznagel/Nelles/Sokol, TKÜV, S. 38.

Für diese Erklärung muss allerdings die alte Gesetzesfassung des TKG herangezogen werden, da in der Neufassung des TKG der „Telekommunikationsdienst für die Öffentlichkeit“ nicht mehr auftaucht.[505] Aber auch die Definition in § 3 Nr. 19 TKG a.F. war für sich betrachtet nicht sehr hilfreich, da hiervon „das gewerbliche Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für beliebige natürliche oder juristische Personen, und nicht lediglich das Angebot für Teilnehmer geschlossener Benutzergruppen“, erfasst wird.

Damit ist für eine aussagekräftige Begriffsdefinition zusätzlich die Berücksichtigung einer geschlossenen Benutzergruppe erforderlich. Eine solche ist dadurch gekennzeichnet, dass sie sich hinreichend bestimmbar von der Allgemeinheit abgrenzen lässt,[506] und dass ihre Teilnehmer in gesellschaftsrechtlichen oder schuldrechtlichen Dauerbeziehungen oder sonstigen nicht-vertraglichen, aber dauerhaften Verbindungen zur Verfolgung gemeinsamer beruflicher, wirtschaftlicher oder hoheitlicher Ziele stehen.[507]

Aus dieser Abgrenzung und Gegenüberstellung zwischen „geschlossener Benutzergruppe“ und „Telekommunikationsdienst für die Öffentlichkeit“ ergibt sich letztendlich, dass letzterer vorliegt, wenn er einer Allgemeinheit zur Verfügung gestellt wird.

[505] Einige Regelungen in der Neufassung des TKG nehmen allerdings nach wie vor Bezug auf den Telekommunikationsdienst für die Öffentlichkeit. Vgl. §§ 3 Nr. 8, § 6 Abs. 1, 78 Abs. 1, 86 Abs. 1, 109 Abs. 2 und Abs. 3, 110 Abs. 1, 112 Abs. 1, 114 Abs. 1, 134 Abs. 2 Nr. 2, 144 Abs. 1 TKG.

[506] Siehe Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 31 mit dem Hinweis, dass „für die Öffentlichkeit“ bedeutet, dass ein gewerbliches Angebot von Telekommunikation für beliebige natürliche oder juristische Personen vorliegen muss (und nicht lediglich für Teilnehmer geschlossener Benutzergruppen). Vgl. auch Schütz in: TKG-Kommentar (2. Auflage), § 6 TKG Rn. 29; Schütz in: TKG-Kommentar (3. Auflage), § 6 TKG Rn 49 ff.; derselbe auch in BB 1996, 1445, 1448, der anmerkt, dass für eine geschlossene Benutzergruppe nicht ausreichend ist, wenn der Zweck so allgemein ist, dass eine Gleichsetzung mit der Allgemeinheit erfolgen müsste. Siehe auch § 6 Abs. 3 Telekommunikations-Verleihungsverordnung vom 19.10.1995 (BGBl. I S. 1434). Der Begriff der „geschlossenen Benutzergruppe ist in §§ 4, 6 Telekommunikations-Verleihungsverordnung definiert (siehe insgesamt zur Telekommunikations-Verleihungsverordnung auch Simon, ArchivPT 1996, 142 ff.). Obwohl diese zum 31.12.1997 außer Kraft getreten ist (§ 38 Telekommunikations-Verleihungsverordnung), können ihre Bestimmungen immer noch zur Auslegung des TKG herangezogen werden, so auch die Definitionen zur geschlossenen Benutzergruppe (siehe hierzu auch Schütz in: TKG-Kommentar (2. Auflage), § 6 TKG Rn. 28 sowie Schütz in: TKG-Kommentar (3. Auflage), § 6 TKG Rn 49 ff.). Zur geschlossenen Benutzergruppe finden sich außerdem Ausführungen bei Tettenborn, MMR 1999, 516, 518; Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 88. Zimmer, CR 2003, 893, 894 nennt als typisches Beispiel einer geschlossenen Benutzergruppe die firmeninterne Kommunikation über W-Lan.

[507] Vgl. Trute/Spoerr/Bosch, TKG-Kommentar, § 3 TKG Rn. 85; siehe auch § 6 Abs. 2 Telekommunikations-Verleihungsverordnung.

Für die datenschutzrechtliche Prüfung im dritten und vierten Abschnitt dieser Arbeit ist jedoch nicht nur entscheidend, inwiefern bei einem VPN eine Telekommunikationsdienstleistung für die Öffentlichkeit und die Anwendbarkeit der TKÜV in Betracht kommen kann. Zu berücksichtigen ist, dass gemäß § 3 Abs. 2 TKÜV die Vorschriften des § 100b Abs. 3 Satz 1 StPO, des § 2 Abs. 1 Satz 3 des G-10-Gesetzes und des §§ 23 a Abs. 8 des Zollfahndungsdienstegesetzes unberührt bleiben und Diensteanbieter daher auf Anordnung Auskunft über die näheren Umstände der Telekommunikation zu erteilen haben.[508]

Hierbei ist zudem nicht nur die Überwachung des Inhalts der Kommunikation zu ermöglichen, sondern es sind ebenso die Verkehrsdaten § 3 Nr. 30 TKG auf Anordnung gemäß §100g und § 100h StPO von dem Diensteanbieter herauszugeben.[509]

Jeder Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, muss darüber hinaus die Pflichten des § 113 Abs. 1 TKG beachten und den zuständigen Stellen unverzüglich Auskunft über die nach §§ 95, 111 TKG erhobenen Daten, also die Grunddaten/Bestandsdaten des Vertragsverhältnisses,510 erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist.[511]

---

[508] Vgl. Holznagel/Enaux/Nienhaus, Telekommunikationsrecht, Rahmenbedingungen – Regulierungspraxis, Rn. 708.

[509] Vgl. Rieß in: Roßnagel, Handbuch Datenschutzrecht, 7.4 Rn. 79; Bäumler in: Roßnagel, Handbuch Datenschutzrecht, 8.3 Rn. 56.

[510] Siehe zu den personenbezogenen Daten die Ausführungen auf S. 92 ff.

[511] Vgl. auch Bäumler in: Roßnagel, Handbuch Datenschutzrecht, 8.3 Rn. 58 und den dortigen Ausführungen zu § 90 TKG a.F., wonach die Anbieter von Telekommunikationsdienstleistungen verpflichtet sind, den Sicherheitsbehörden einen direkten Zugriff auf ihre Kundendateien zu eröffnen.

IV. Zusammenfassung

Die wesentlichen Ausführungen dieses zweiten Abschnitts werden nochmals als Basis für die im dritten und vierten Abschnitt folgende rechtliche Prüfung wie folgt in Kürze zusammengefasst:

Bei einem VPN handelt es sich um einen kombinierten Online-Dienst. Für die umfassende datenschutzrechtliche Prüfung ist dieser Dienst sowohl in seine einzelnen Bestandteile/Dienstleistungen als auch in die einzelnen betroffenen Personenkonstellationen im Sinne einer dienstorientierten Betrachtungsweise im Mehrpersonenverhältnis aufzugliedern.

Für die notwendige Abgrenzung der einzelnen beteiligten Personen eines VPN sind Definitionen aufgestellt worden, wobei in dieser Arbeit zwischen Provider, VPN-Auftraggeber, Nutzer und Betroffener unterschieden wird.

Aufgrund der abstrakten Betrachtung des Begriffs „Online-Dienstes“ als wirtschaftliche Tätigkeit, die im Internet erbracht wird, kann unter dem Oberbegriff dieser Arbeit „Online-Dienste und Datenschutz“ im dritten und vierten Abschnitt sowohl der Datenschutz gegenüber Personen geprüft werden, die den Dienst nicht selbst in Anspruch nehmen (Betroffener). Diese Betrachtungsweise ermöglicht aber auch die Sichtweise, dass der Nutzer eines VPN gleichzeitig Anbieter eines VPN für andere (Nutzer) sein kann.

Im Rahmen der datenschutzrechtlichen Prüfung ist Exklusivitätsverhältnis zu beachten, so dass die Regelungen des BDSG jeweils nur subsidiär zur Anwendung gelangt.

3. Abschnitt
Dienste im VPN und Datenschutz

In diesem Teil steht das „Dienstverhältnis VPN“ zwischen einem jeweiligen Anbieter und Nutzer im Fokus der Betrachtung. Es werden diejenigen Personenverhältnisse und Dienstleistungen geprüft, die im unmittelbaren Zusammenhang mit der Nutzung des VPN stehen. Hierbei sind Daten betroffen, die durch die aktive Nutzung des (jeweiligen) Dienstes im Hinblick auf den (jeweiligen) Nutzer entstehen.

Bei den relevanten Dienstleistungen eines VPN handelt es sich im Einzelnen um die bereits im zweiten Abschnitt „Technischen Grundlagen“ dargestellten Bestandteile eines VPN:

- (Herstellen einer) Internetverbindung,[512]
- Zwangsweises Tunneling,[513]
- VPN-Kommunikation[514] sowie
- Zusatzdienst E-Mail.[515]

Diese (Einzel-)Dienstleistungen des kombinierten Dienstes „VPN“ stellt der Provider dem VPN-Auftraggeber zur Nutzung bereit, und dieser stellt die einzelnen Leistungen wiederum (weiteren) Nutzern zur Verfügung. Demzufolge sind insgesamt die Personenverhältnisse zwischen „Provider und VPN-Auftraggeber“, zwischen „VPN-Auftraggeber und Nutzer des VPN“ sowie zwischen „Provider und Nutzer des VPN“ rechtlich zu betrachten.

[512] Siehe S. 19.
[513] Siehe S. 57.
[514] Siehe S. 43 ff..
[515] Siehe S. 62.

A. Provider – VPN-Auftraggeber

I. Rechtliche Einordnung der Dienste im VPN

Bei den einzelnen Dienstleistungen wird zunächst untersucht, ob diese in dem hier untersuchten Rechtsverhältnis zwischen Provider und VPN-Auftraggeber rechtlich als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG oder als Teledienst gemäß § 2 Abs. 1 TDG einzuordnen sind.
Entsprechend der bereits im zweiten Abschnitt (Technische Grundlagen) dargestellten Reihenfolge wird nachfolgend ebenso als erster Prüfungspunkt die „Internetverbindung“ in rechtlicher Hinsicht betrachtet.[516]

1. Internetverbindung

Unter dem gleichnamigen Punkt „Internetverbindung“ wurde im zweiten Abschnitt („Technische Grundlagen“) dargestellt, dass zum Aufbau einer Internet-Verbindung wiederum verschiedene Dienste erforderlich sind. Hierzu zählen die Bereitstellung des Internetzugangs durch einen Anbieter (=Access-Providing) sowie (regelmäßig) die Bereitstellung einer Telekommunikationsleitung durch einen Carrier.[517]
Darüber hinaus müssen DNS-Service und Routing zur Verfügung gestellt werden.[518]

Zu betonen ist, dass die nachfolgenden Ausführungen (bezüglich Access-Providing, TK-Providing, Routing und DNS-Service) für sämtliche Nutzer und Teilnehmer einer Internetverbindung und nicht VPN-spezifisch gelten. Etwas anderes gilt nur, soweit im Verlauf der Prüfung eine Besonderheit in einem VPN hervorgehoben wird. Dies betrifft gleichermaßen die anschließende datenschutzrechtliche Prüfung.[519]

[516] Siehe S. 19.
[517] Siehe S. 19 ff.
[518] Siehe S. 30 ff.
[519] Siehe die datenschutzrechtliche Prüfung auf S. 162 ff.

a. Bereitstellung von Internetzugangsknoten/Access-Providing

Eine Teilleistung des Providers eines VPN ist die Bereitstellung des Internetzugangs (Access-Providing), so dass er insoweit ein Access-Provider ist.[520]

Beim Access-Providing besteht die Hauptleistung eines Providers darin, dem Vertragspartner die Nutzung des Internet zu ermöglichen, den Internetzugang einzurichten und bereit zu halten.[521] Für den Zugang in das Internet ist neben der Einrichtung und Unterhaltung von Internetzugangsknoten[522] regelmäßig die Bereitstellung einer Software seitens des Anbieters, oftmals gepaart mit einer Passwortvergabe erforderlich.[523]

Access-Providing wird regelmäßig als typischer Telekommunikationsdienst gemäß § 3 Nr. 24 TKG betrachtet.[524]

---

[520] Siehe hierzu im technischen Teil die Ausführungen auf S. 29 ff.

[521] Vgl. Cichon, Internetverträge,Rn. 34.; Eichhorn, Internet-Recht, S. 67; Koch, Internet-Recht, S. 8; Freytag, Haftung im Netz, S. 223 ff.; Wimmer/Michael, Der Online-Provider im neuen Multimediarecht, S. 51; Pernice, DuD 2002, 207, 209; Riehmer/Hessler, CR 2000, 170, 171; Spindler, K&R 1999, 488, 489; Wischmann, MMR 2000, 461, 461; Härting, CR 2001, 37, 38; Kloepfer, Informationsrecht, § 13 Rn. 29. Siehe auch Schrey/Meister, K&R 2002, 177. 181 Fn. 38, die die Auffassung vertreten, dass ein Access-Provider keine eigenen Netze betreibt, sondern nur den Zugang zu den Netzen vermittelt. Diese Meinung schränkt jedoch den Begriff des Access-Providers zu sehr ein, da dies im Umkehrschluss bedeuten würde, dass beispielsweise AOL keine Access-Leistungen (mehr) anbietet, da AOL seit Frühjahr 1998 seinen Zugang bundesweit über ein eigenes Netz anbietet und dabei Online- und Telefongebühren gemeinsam verrechnet (siehe hierzu Voss, Das große Internet & PC Lexikon 2004, „AOL“ S. 74). Vgl. auch Petri/Göckel, CR 2002, 329, 330 Fn. 4, die darlegen, dass Access-Provider meist über ein eigenes Netz verfügen.

[522] Vgl. auch Schaar, Datenschutz im Internet. Rn. 22, der darlegt, dass die primäre Aufgabe eines Access-Providers darin besteht, Zugangsknoten bereit zu halten, die von den Nutzern aus öffentlichen Telekommunikationsnetzen angewählt werden können.

[523] Vgl. zum Internetzugang auch Kröger/Kuner, Internet für Juristen, S. 6; Kröger/Göers/Hanken, Internet für Juristen, S. 13; Kroiß/Schuhbeck, Jura Online, S. 5 ff; Schneider, Verträge über Internet-Access, S. 95.

[524] LG Darmstadt CR 2006, 249, 250; OVG Nordrhein-Westfalen CR 2003, 361, 364; OLG Hamburg CR 2000, 363, 364; OLG Hamburg MMR 2000, 278, 279; OLG Hamburg MMR 2000, 611, 613; AG Wiesbaden MMR 2002, 563, 563; siehe auch Moos, CR 2003, 385, 386, der die Einordnung des Access-Providing als herrschende Auffassung bezeichnet. Siehe ebenso Grote, BB 1998, 1117, 1118; Anmerkung Schmitz zu LG Potsdam, CR 2000, 123, 125; Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 78/85, Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 86/87; Koenig/Loetz, CR 1999, 438, 440; Stadler, MMR 2002, 343, 344; Moos in: Kröger/Gimmy, Handbuch zum Internetrecht, S. 510; Gottschalk in: Kaminski/Henßler/Kolaschnik/Papathoma-Baetge, Rechtshandbuch E-Business, S. 713; Kloepfer, Informationsrecht, § 13 Rn. 43; Gounalakis/Rhode, Persönlichkeitsschutz im Internet, Rn. 290; vgl. außerdem Spindler/Volkmann, K&R 2002, 398, 399 mit der Ausführung, dass Access-Providing keine inhaltliche Komponente, sondern nur den Transport von Daten umfasst. Siehe auch Bleisteiner, Rechtliche Verantwortung im Internet, S. 111, der zwischen „Zugang zur Nutzung“, „Angebot zur Nutzung“ und „genutzten Inhalt“ unterscheidet, und den „Zugang zur Nutzung“ der Telekommunikation zuordnet. A.A. Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I

Hiervon abweichend gibt es jedoch die Auffassung, dass es sich bei der Vermittlung eines Zugangs in das Internet nicht um einen Telekommunikationsdienst, sondern um einen Teledienst oder sogar um einen Mediendienst[525] handelt.[526]
Dieser Auffassung kann nicht gefolgt werden, wie die folgenden Ausführungen zeigen.

Rn. 49; Beck-IuKDG-Tettenborn, § 2 TDG Rn. 77; Kröger/Moos, AfP 1997, 675, 679; Schaar, Datenschutz im Internet, Rn. 262; Beucher/Leyendecker/v. Rosenberg, Mediengesetze-Kommentar, § 2 TDG Rn. 6; Rasmussen, CR 2002, 36, 38; siehe auch Röhrborn/Katko, CR 2002, 882, 887 (für lokale Funknetzwerke „W-Lan") die § 2 Abs. 2 Nr. 3 TDG anwenden und davon ausgehen, dass es sich bei einem Internetzugang mittels W-Lan-Technik um einen Teledienst handelt (a.A. Zimmer, CR 2003, 893, 893, die die Nutzung von W-Lan unter den Begriff der Telekommunikation subsumiert); siehe auch Pankoke, Von der Presse- zur Providerhaftung, S. 41/56, der zwar einerseits von einer Telekommunikationsdienst(-leistung) ausgeht, aber andererseits aufgrund der von ihm monierten unklaren Gesetzesfassung keine endgültige Einordnung vornimmt.

[525] Zum Mediendienst siehe Fn. 33.

[526] Dix, DuD 2003, 234, 235; Heidrich, DuD, 237, 237; Engel, MMR-Beilage 4/2003, S. 2 ff.; siehe auch Neubauer in: Moritz, Rechts-Handbuch zum E-Commerce, D Rn. 27, der zwar einerseits darauf hinweist, dass Access-Providing zumindest zum Teil Telekommunikation darstellt, aber andererseits unter Berufung auf § 3 Nr. 1 TDG die Haftungsprivilegierung des § 9 TDG anwendet. Das VG Düsseldorf (VG Düsseldorf, CR 2003, 384, 384) hat zwar die Einordnung eines Access-Providers als Teledienst-Anbieter oder Mediendienst-Anbieter offen gelassen, jedoch die Anwendbarkeit des TKG für Access-Provider verneint, siehe hierzu Anmerkung Dieselhorst zu VG Düsseldorf, ITRB 2003, 194,195. Diese Entscheidung ist eines von 17 Eilverfahren, die sich allesamt auf den gleichen Sachverhalt gründen, da die Bezirksregierung Düsseldorf im Februar 2003 Verfügungen gegen 80 Zugangsprovider erlassen hat, nach denen die Anbieter den Zugang zu zwei US-amerikanischen Websites mit nationalsozialistischen Inhalten sperren mussten. Nach Erhebung von Widersprüchen hatte die Bezirksregierung jeweils die sofortige Vollziehbarkeit der Verfügungen angeordnet, gegen die sich mehrere Provider vor Gericht wehrten. So hat das OVG Nordrhein-Westfalen die Verfügungen der Bezirksregierung Düsseldorf vorläufig bestätigt. Das OVG Nordrhein-Westfalen hatte über die Beschwerde gegen den Beschluss des VG Arnsberg zu entscheiden hatte (siehe hierzu auch den Beschluss des OVG Nordrhein-Westfalen, CR 2003, 361 ff., in welchem festgestellt wird, dass Maßnahmen zur Sperrung auch gegen einen Access-Provider als Diensteanbieter von fremden Inhalten nach § 7 MDStV gerichtet werden können, wenn Webseiten offenkundig unzulässige Inhalte nach § 12 MDStV enthalten und Maßnahmen gegenüber dem bzw. den Verantwortlichen nach § 6 MDStV nicht durchführbar bzw. nicht erfolgversprechend sind; siehe hierzu ebenso Feldmann, ITRB 2003, 118, 118 sowie Volkmann, Anmerkung zu VG Düsseldorf, CR 2005, 885, 893). Außerdem waren das VG Minden, das VG Düsseldorf sowie das VG Köln mit dieser Frage befasst (siehe VG Düsseldorf, CR 2003, 384, 384; VG Minden, CR 2003, 384, 384; Feldmann, ITRB 2003, 22, 23 zum Beschluss des VG Minden; vgl. Dieselhorst, ITRB 2003, 194, 195 zum Beschluss des VG Düsseldorf). Vgl. auch Engel, MMR-Beilage 4/2003, 1, 5, 13, der zum einen die grundsätzliche Argumentation des Regierungspräsidiums Düsseldorfs zur Anwendbarkeit des MDStV, insbesondere von § 22 Abs. 3 MDStV auf Access-Provider kritisiert und insgesamt die Verfügung des Regierungspräsidiums Düsseldorfs als rechtswidrig einstuft, zum anderen aber den Access-Provider gemäß § 2 Abs. 2 Nr. 3 TDG als Teledienst-Anbieter einordnet (Engel aaO).

aa. Abgrenzung zum Internet-Dienst

Zur Klarstellung sei erst einmal festgestellt, dass es sich beim Access-Providing um eine Dienstleistung handelt, und Access-Providing nicht unter den Begriff des Internet-Dienstes (im Sinne eines Werkzeugs zur Kommunikation bzw. Kommunikationsmöglichkeit[527]) fällt.

Eine kurze Ausführung hierzu empfiehlt sich, da die Auffassung vertreten wird, dass Access-Provider selbst keine Dienstleistung erbringen, die über das Internet erbracht wird, sondern selbst das Netz bilden.[528]

Nach Ansicht der EU-Kommission handelt es sich bei dem Access-Providing jedoch um einen Dienst der Informationsgesellschaft.[529] Dieses (richtige) Verständnis der EU-Kommission kann man leicht damit begründen, dass zwar die eigentümliche Struktur des Internet seitens der Provider genutzt wird, aber die Provider selbst nicht unbedingt das Netz repräsentieren bzw. darstellen. Ein Provider schafft erst bei den einzelnen Nutzern die Voraussetzung dafür, diese eigentümliche Struktur des Internet nutzen zu können. Dies geschieht in der Regel mittels einer auf dem Rechner des Nutzers zu implementierenden Software und/oder mittels Passwortvergabe,[530] so dass man insgesamt festhalten kann, dass Access-Provider Dienste zur Nutzung der verschiedenen Internet-Dienste[531] und der Online-Dienste[532] anbieten, aber nicht selbst das Netz bilden.

Daher kann man zu Recht feststellen, dass es sich bei dem Access-Provider um einen Online-Dienst-Anbieter[533] handelt, da er eine wirtschaftliche Tätigkeit erbringt, die im Internet erbracht wird und die in der Vermittlung zum Internet besteht.

---

[527] Siehe oben S. 75 ff.
[528] Vgl. Hoeren, MMR 1999, 192, 194; Spindler, MMR-Beilage 7/2000, 4, 5.
[529] Siehe Artikel 13 des Vorschlages über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt vom 18.11.1998, KOM (1998) 586 endg. Vgl. auch Glatt, Vertragsschluss im Internet, S. 73; Spindler, MMR-Beilage 7/2000, 4, 5. Siehe außerdem Fn. 304.
[530] Vgl. außerdem Kröger/Kuner, Internet für Juristen, S. 6.
[531] Siehe S. 75 ff.
[532] Siehe S. 64 ff.
[533] Insoweit scheint daher die Definition von Koch, CR 1997, 193, 197 als zu eng, der als Betreiber von Online-Diensten ansieht, wer eigene Dienste betreibt und in diesen Diensten eigene, überwiegend aber fremde Inhalte anbietet.

Dies gilt selbst dann, wenn ein Provider über ein eigenes Netz verfügen sollte.[534] In diesem Falle stellt er gleichermaßen den Internetzugang bereit und erbringt dadurch gegenüber dem Nutzer eine Dienstleistung. Das Netz des Providers ist zwar Teil einer Netzstruktur, so dass auch der Provider (abstrakt betrachtet) Teil des Internets ist. Aber er ist nach wie vor ein Netz**betreiber** und damit ein Dienstleister.

bb. Abgrenzung zum Teledienst

aaa. Datenübertragungsfunktion

Das Client-Server-Prinzip[535] vermag bei der Abgrenzung zwischen Telekommunikationsdienst und Teledienst keinen zuverlässigen Anknüpfungspunkt für deren Einordnung bilden. Zwar wird die Auffassung vertreten, dass stets bei einem Angebot, das auf dem Client-Server-Prinzip basiert und dem die redaktionelle Gestaltung fehlt, ein Teledienst gegeben ist.[536] Dass dies in dieser Pauschalität nicht stimmen kann, zeigt aber, dass anderenfalls im Zusammenhang mit dem Internet überhaupt nicht mehr über Telekommunikationsdienste diskutiert und ohne weiteres das TDG zur Anwendung gelangen müssteda sämtliche Dienstleistungen im Internet auf diesem Prinzip beruhen. Dies würde bedeuten, dass selbst die Dienstleistung des Access-Providing, die nach überwiegender Meinung einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG darstellt,[537] nun zum Teledienst „mutieren“ müsste. Denn auch beim Aufbau einer Internetverbindung ruft ein Client einen Server (Internetzugangsknoten) an, um „ins Internet“ weitervermittelt zu werden.[538]

---

[534] Siehe zum Begriff des Backbone S. 28.
[535] Siehe hierzu S. 43.
[536] Spindler in: Roßnagel, Recht der Multimedia-Dienste, § 2 TDG Rn. 82 f.. Vgl. in diesem Sinne ebenso Holznagel/Kibele in Hoeren/Sieber, Teil 5 Rn. 68, die ausführen, dass Internet-Dienste nach dem Client-Server-Prinzip (www, gopher, telnet, ftp) dem Nutzer ermöglichen, einen Dienst zu empfangen und Abrufdienste gemäß § 2 Abs. 2 Nr. 4 MDStV darstellen, da sie an eine beliebige Öffentlichkeit gerichtet sind. Siehe auch Kröger/Moos, ZUM 1997, 462, 466 ff., insbesondere S. 467; Kröger/Moos, AfP 1997, 675, 679, verweisen darauf, dass alle Internet-Dienste aufgrund des Client-Server-Prinzips als Tele- oder Mediendienste einzustufen sind. Ebenso Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I, Rn. 56, der darauf verweist, dass alle „Internet-Dienste“ auf dem Client-Server-Prinzip beruhen.
[537] Siehe S. 122.
[538] Siehe S. 32

Die Abgrenzung zwischen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG und Teledienst gemäß § 2 Abs. 1 TDG lässt sich aber unmittelbar aus den einschlägigen Normen des TKG und des TDG ableiten: Das TKG gilt für den technischen Vorgang der Übertragung von Inhalten gelten,[539] während sich das TDG auf die übertragenen Inhalte bezieht.[540]

So kommt gemäß § 3 Nr. 24 TKG das TKG für Vorgänge zur Anwendung, die ohne nach dem Inhalt zu unterscheiden **anwendungsdiensteunabhängig** die Übertragung der Nachrichten und die Verständigung zwischen Sender und Empfänger regeln.[541]
Gemäß § 2 Abs. 1 TDG bezieht sich das Teledienstegesetz hingegen auf Vorgänge, welche **anwendungsspezifisch** Darstellung, Inhalt oder Anwendung der übertragenen Daten regeln.[542] Bei diesen Inhalten handelt es sich um Informationen oder Daten, die der Anbieter regelmäßig auf seinem Server bereithält.[543]

Betrachtet man den im technischen Teil beschriebenen Einwahlvorgang ins Internet,[544] dann liegt der hauptsächliche Bezugspunkt darin, dass überhaupt eine Verbindung in das Internet zustande kommt und Daten übertragen und/oder abgerufen werden können: Der Nutzer (Client) ruft den Internetzugangsknoten (Server) an, um mit dem Internet verbunden zu werden. Die Dienstleistung des Access-Providers, die notwendigen technischen Voraussetzungen, insbesondere den Internetzugangsknoten, für die Datenübertragung bereit zu stellen, ist Grundvoraussetzung, um den Nutzer zu ermöglichen, Teledienste, Mediendienste oder gegebenenfalls weitere

[539] Telekommunikation ist gemäß § 3 Nr. 22 TKG der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen.
[540] Siehe die Ausführungen auf S. 66 ff. Außerdem: OLG Hamburg, CR 2000, 363, 364; Stögmüller in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 95; Tettenborn, MMR 1999, 516, 518; Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2983; Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 109; Beck-IuKDG-Tettenborn, § 2 TDG Rn. 46; Eichhorn, Internet-Recht, S. 35/36/39 (Tabelle); Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 70.
[541] Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 75.
[542] Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 75; Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 24.
[543] In § 2 Abs. 2 TDG findet sich der Beispielkatalog für Teledienste, worunter auch etwa Werbebanner als Angebote zur Information und Kommunikation im Sinne von § 2 Abs. 2 Nr. 2 TDG fallen sollen (vgl. hierzu Pankoke, Von der Presse- zur Providerhaftung, S. 78 ff.).
[544] Siehe S. 32.

Telekommunikationsdienste in Anspruch nehmen zu können. Diese Bereitstellung erfolgt dementsprechend anwendungsdiensteunabhängig. Auch dem Access-Providing liegen Internet-Dienste zugrunde, die jedoch unterschiedlich von dem angestrebten Einsatz des Nutzers sind. So kann die Bereitstellung eines Internetzugangs mit einer Datenübertragung mittels ftp, http, smtp genauso gut zusammenhängen wie mit der Ermöglichung des Internet-Chats mittels des Protokolls IRC.[545]

Der Dienst des Access-Providing wird ebenso wenig aufgrund der Vergabe einer IP-Adresse für den Einwahlvorgang zu einem Teledienst.[546]
Im IuKDG-Bericht der Bundesregierung[547] sind zwar die IP-Adressen den Nutzungsdaten[548] des § 6 TDDSG zugeordnet worden,[549] und es wird des Weiteren die Auffassung vertreten, dass es sich bei der Vergabe einer IP-Adresse um einen Teledienst handelt.[550] Richtigerweise besteht aber kein zwingender Zusammenhang zwischen IP-Adresse und Teledienst. Hiergegen spricht, dass die Vergabe von IP-Adressen in keiner Weise auf Teledienste begrenzt ist. Für die Nutzung des Internets bzw. von dessen Angeboten eine IP-Adresse notwendig, [551] und zwar als unerlässliche Voraussetzung sogar bereits für den Aufbau einer Verbindung.

Es empfiehlt sich nicht, den Vorgang der Vergabe der IP-Adresse von dem Vorgang des Internet-Access „künstlich“ abzutrennen,[552] da die Vorgänge des „Internetzugangs“ und die „Vergabe der IP-Adresse“ vielmehr untrennbar

---

[545] Siehe hierzu auch S. 75 ff. sowie das Bildbeispiel zur E-Mail-Kommunikation S. 63.
[546] Vgl. auch Dix, DuD 2003, 234, 235; Heidrich, DuD 2003, 237, 237/238.
[547] Bundestag-Drucksache 14/1191.
[548] Nach Ansicht der Regierung handelt es sich bei Nutzungsdaten im Sinne des § 6 TDDSG um solche personenbezogenen Daten, die für die Nutzung der Netzinhalte notwendig sind oder damit im Zusammenhang stehen, z.B. IP-Adresse, Name Service, Routing. Diese seien jedoch nicht mit dem in § 5 TDSV geregelten Katalog der Verbindungsdaten deckungsgleich (siehe Bundestag-Drucksache 14/1191, S. 15).
[549] Dadurch war geplant, eine klare Abgrenzung zwischen den Nutzungsdaten im Sinne des TDDSG und den Verbindungsdaten im Sinne der Telekommunikationsdatenschutzverordnung (TDSV) zu schaffen (siehe Bundestag-Drucksache 14/1191, S. 15).
[550] Tettenborn, MMR 1999, 516, 518; Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 75/83; siehe auch Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 74;
[551] Siehe S. 21 ff.
[552] So aber auch: Holznagel/Kibele in: Hoeren/Sieber, Teil 5 (ab der 6. Ergänzungslieferung) Rn. 72 und Schaar, Datenschutz im Internet, Rn. 262.

miteinander verbunden sind.[553] Der Internetzugang bzw. Access ist ein Telekommunikationsdienst und benötigt hierfür als unbedingte technische Voraussetzung IP-Nummern.[554]

Daher wäre es nicht folgerichtig, die Vergabe der IP-Adresse bzw. den Vorgang der Vergabe der IP-Adresse separat als Telekommunikationsdienst[555] oder als Teledienst[556] einzuordnen. Eine andere Beurteilung ergibt sich ebenso wenig aus den Ausführungen der Bundestag-Drucksache 14/1191.[557]Hier wird zwar die Vergabe der IP-Adresse als Teledienst eingestuft. Aus dem Gesamtzusammenhang ergibt sich aber, dass mit der Vergabe der IP-Adresse die Bereitstellung eines Internetzugangs den Access-Provider gemeint ist, und zwar in Abgrenzung zu demjenigen Provider, der die Telefonleitung bereitstellt. Dort wird ausgeführt, dass für die Möglichkeit, im Internet zu surfen, neben dem Aufbau einer ständigen Verbindung über die Telefonleitung, die Vergabe einer IP-Adresse, (Domain-)Name-Service und Routing erforderlich ist. Dies bedeutet aber nichts anderes, als dass neben einem TK-Provider auch ein Access-Provider erforderlich ist. Denn letzterer ist für die Vergabe der IP-Adresse als unerlässliche Voraussetzung des Internetzugangs „zuständig“.

---

[553] Dies ändert natürlich nichts an der Tatsache, dass im Verhältnis zwischen einem Nutzer und einem Telediensteanbieter, etwa bei Zugriff auf eine Website, die IP-Adresse ebenso ein Nutzungsdatum gemäß § 6 TDDSG darstellen kann. Hier kann also keine pauschale Einordnung als Verkehrsdatum im Sinne von § 3 Nr. 30 TKG oder Nutzungsdatum gemäß § 6 TDDSG vorgenommen werden.

[554] Siehe Bundestag-Drucksache 14/1191, S. 7.

[555] In diesem Sinne aber wohl Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 41; vgl. auch Holznagel, MMR 2003, 219 ff., der IP-Nummern als Nummer im Sinne von § 3 Nr. 10 TKG bewertet.

[556] Vgl. aber Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 96; Tettenborn, MMR 1999, 516, 518; siehe außerdem die Nachweise bei Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 41 Fn. 2.

[557] Siehe Bundestag-Drucksache 14/1191, S. 7.

bbb. Abgrenzung zum Angebot zur Nutzung des Internet

Aus den gerade gemachten Ausführungen ergibt sich ebenso, dass es sich beim Access-Providing auch nicht um ein Angebot im Sinne von § 2 Abs. 2 Nr. 3 TDG zur Nutzung des Internet handelt. Denn bei der „reinen“ Zugangsvermittlung stehen gerade keine inhaltlichen Angebote im Vordergrund, sondern die Transportfunktion als Voraussetzung für die Inanspruchnahme von Tele- oder Mediendiensten oder (weiteren) Telekommunikationsdiensten.[558]´Es geht hier vielmehr vorrangig darum, dass der Server bzw. Internetzugangsknoten des Providers funktionstüchtig ist, also um die Verständigung zwischen Sender und Empfänger sowie dem (Weiter-) Transport von Inhalten.

Wie sich weiterhin aus der Abgrenzung zwischen Transport- und Inhaltsebene[559] ergibt, ist folgerichtig bei sämtlichen Telediensten im Sinne von § 2 TDG und damit auch § 2 Abs. 2 Nr. 3 TDG das Bereithalten[560] von eigenen oder fremden Inhalten bzw. Informationen[561] auf dem Server des Providers erforderlich.[562]
Eine solche Auslegung ergibt sich im Übrigen unmittelbar aus dem Gesetz. Denn gemäß § 3 Nr. 1 1. Alt. TDG halten Telediensteanbieter im Sinne von § 2 Abs. 2 TDG Angebote zur Nutzung bereit. Damit erfolgt insbesondere eine klare

[558] Vgl. hierzu auch die folgenden Ausführungen zu „ftp“ S. 305 ff.
[559] Vgl. hierzu auch Tettenborn, MMR 1999, 516, 518; Krager in: Königshofen, Das neue Telekommunikationsrecht in der Praxis, S. 119.
[560] Siehe zum Begriff des Bereithaltens Sieber in: Hoeren/Sieber, Teil 19 Rn. 288. Danach erfordert das Bereithalten von Inhalten eine Herrschaftsmacht über die einzelnen konkreten Daten. Siehe auch Stögmüller in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 24, wonach das Bereithalten ein nicht nur kurzzeitiges Vorhalten der Inhalte auf dem Server des Providers meint.
[561] In §§ 8 ff. TDG ist nunmehr der Begriff „Inhalt“ durch „Information“ ausgetauscht worden, jedoch ebenso ohne nähere gesetzliche Konkretisierung. Zum Begriff des Inhalts als „Information jeglicher Art in Schrift, Bild und/oder Ton“, mit dem Hinweis, dass dieser gesetzlich nicht näher definiert ist, siehe auch Spindler, NJW 1997, 3193, 3195; Koch, CR 1997, 193, 196/197.
[562] Vgl. insbesondere Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 87 Fn. 459 mit dem Hinweis, dass im Sinne von § 2 Abs. 2 Nr. 3 TDG kein Anbieter oder Access-Provider in Betracht kommen kann, der mit dem Zugang keine Anwendungsdienste, wie z.B. eine eigene Startseite mit Suchdiensten usw., verbindet, sondern nur Telekommunikationsdienstleistungen erbringt. Ebenso Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 44 (wobei hier die Ausführungen bezogen auf das Verhältnis zwischen Arbeitgeber und Arbeitnehmer gemacht worden sind).

Differenzierung zur Zugangsvermittlung gemäß § 3 Nr. 1 2. Alt. TDG.[563] Die Zugangsvermittlung ist grundsätzlich im technischen Sinne zu verstehen und beinhaltet (anders als das Bereithalten im Sinne von § 2 Abs. 2 Nr. 3, § 3 Nr. 1 1. Alt. TDG) kein Angebot an den Nutzer zum Abruf inhaltlicher Daten.[564]

ccc. Abgrenzung zur Zugangsvermittlung

Gemäß dieser Definition, wonach Zugangsvermittlung grundsätzlich technisch zu verstehen ist, könnte der Access-Provider zwar als Telediensteanbieter im Sinne von § 3 Nr. 1 2. Alt. TDG zu verstehen sein,[565] womit das TDDSG zur Anwendung gelangen würde. Dies hätte vor allem wegen der privilegierenden Haftung nach §§ 9 ff. TDG praktische Auswirkungen. Eine parallele Anwendung von TDG und TKG würde aber gleichermaßen die datenschutzrechtlichen Pflichten beeinflussen. Zwar sind §§ 91 ff. TKG und TDDSG teilweise konform gestaltet, zumindest, was die unverzüglichen Löschungspflichten im Hinblick auf entstehende Nutzungs- bzw. Verkehrsdaten und Speicherungsfristen anbelangt.[566] Aber dennoch könnten sich in der Praxis dadurch Unterschiede ergeben, dass § 4 Abs. 1 S. 3 TDDSG dem Provider dem Nutzer gegenüber Unterrichtungspflichten auferlegt, die für diesen zudem jederzeit abrufbar sein müssen. Nutzer ist gemäß § 2 Nr. 2 TDDSG jede natürliche Person, die Teledienste in Anspruch nimmt. Damit wäre also die Frage aufgeworfen, ob der Provider in einem Mehrpersonenverhältnis durch diese Vorschrift verpflichtet

[563] Vgl. hierzu auch Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 78. Insoweit unrichtig ist die Auffassung von Beucher/Leyendecker/v. Rosenberg, Mediengesetze-Kommentar, § 2 TDG Rn. 6, die § 2 Abs. 2 Nr. 3 TDG als Zugangsvermittlung im Sinne von § 3 Nr. 1 2. Alt. TDG begreifen. Denn aus dem gesetzlichen Wortlaut ergibt sich eindeutig, dass § 2 Abs. 2 TDG „Angebote zur Nutzung" erfasst und nicht die Zugangsvermittlung. So spricht auch § 2 Abs. 2 Nr. 3 TDG von einem Angebot zur Nutzung, in dem Falle zur Nutzung des Internet.

[564] Siehe zur technischen Funktion der Zugangsvermittlung: Sieber in: Hoeren/Sieber, Teil 19 Rn. 284; v.Bonin/Köster, ZUM 1997, S. 821, 823 ff.; Bettinger/Freytag, CR 1998, 545, 549, Freytag, ZUM 1999, 185, 192; Anmerkung Schmitz zu LG Potsdam, CR 2000, 123, 125; Pichler, MMR 1998, 79, 87.

[565] Den Access-Provider als Zugangsvermittler im Sinne von § 3 Nr. 1 2. Alt. TDG sehen allerdings: LG München, CR 2000, 117, 119; Anmerkung Schmitz zu LG Potsdam, CR 2000, 123, 125; Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 85; Spindler, ZUM 1999, S. 775, 778/779; Anmerkung Spindler zu OLG Hamburg, MMR 2000, 278, 279;; Waldenberger in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDG Rn. 25 (Access-Provider sind Zugangsvermittler gemäß § 3 Nr. 1 TDG); Koch, Internet-Recht, S. 897; Riehmer/Hessler in: Spindler, Vertragsrecht der Internet Provider (1. Auflage), Teil II Rn. 173; vgl. auch Bleisteiner, Rechtliche Verantwortung im Internet , S. 111 ff.; Wimmer/Michael, Der Online-Provider im Multimediarecht, S. 57; zur Anwendbarkeit von § 3 Nr. 1 2. Alt. TDG für den Backbone-Betreiber bzw. Access zum Backbone siehe Petri/Göckel, CR 2002, 418, 421.

[566] Vgl. Röhrborn/Katko, CR 2002, 882, 887, die darauf hinweisen, dass im Vergleich zum Telekommunikationsdatenschutz keine fundamentalen Unterschiede bestehen.

wäre, nicht nur seinen Vertragspartner als Teilnehmer (§ 3 Nr. 20 TKG) über die Verwendung von personenbezogenen Daten aufzuklären (§ 93 TKG), sondern gemäß § 4 Abs. 1 TDDSG darüber hinaus die Nutzer selbst, und zwar durch jederzeit abrufbare Informationen.

Eine Auseinandersetzung mit dieser Frage erübrigt sich allerdings, da die Regelung des § 2 Abs. 4 Nr. 1 TDG Telekommunikationsdienstleistungen ausdrücklich von dem Anwendungsbereich des TDG ausschließt. Daraus folgt, dass das TKG und nicht das TDDSG einschlägig ist.[567]
Unbenommen ist zwar, dass die Haftungsregelungen bzw. Haftungsprivilegierungen des TDG (§§ 9 ff. TDG) aus Gründen der Angemessenheit auch für den Access-Provider Geltung beanspruchen sollten. Argumentiert wird diesbezüglich, dass der Gesetzgeber nicht gewollt habe, dass Telekommunikationsdienstleistungen vom Anwendungsbereich des TDG, insbesondere von dessen Haftungsprivilegierungen[568], ausgeschlossen sind.[569] Insbesondere, so lautet die weitere Begründung, wäre bei wörtlicher Anwendung des § 2 Abs. 4 Nr. 1 TDG den Haftungsvorschriften jeglicher Anwendungsbereich entzogen.[570]
Dieses Argument berücksichtigt jedoch zum einen nicht die funktionale Trennung zwischen Transport- und Inhaltsebene:[571] Obgleich jeder Teledienst

[567] Vgl. Moos, CR 2003, 385, 386, der ebenfalls wegen der ausdrücklichen Regelung in § 2 Abs. 4 Nr. 1 TDG davon ausgeht, dass für das Access-Providing allein telekommunikationsrechtliche Vorschriften maßgeblich sind und parallel nicht das TDG bzw. TDDSG zur Anwendung gelangt.
[568] Die Verantwortlichkeit wurde vor der Einführung des Gesetzes zum elektronischen Geschäftsverkehr (EGG) und der damit verbundenen Änderungen des TDG stets an § 5 TDG a.F. gemessen (siehe zum EGG Fn. 27). Einschlägig sind nach der Gesetzesneufassung nunmehr §§ 8 bis 11 TDG. Siehe auch Köhler/Arndt/Fetzer, Recht des Internet, S. 257 zu § 9 TDG und § 5 TDG a.F. und Gounalakis/Rhode, Persönlichkeitsschutz im Internet, Rn. 290, die darauf hinweisen, dass § 5 Abs. 3 TDG a.F. durch § 9 TDG ersetzt worden ist und nunmehr für den Access-Provider § 9 TDG Geltung beanspruchen muss. Vgl. zu § 9 TDG und der Geltung für den Access-Provider auch Schaar, Datenschutz im Internet, Rn. 305.
[569] Siehe Pankoke, Von der Presse- zur Providerhaftung, S. 38, jedoch ohne entsprechenden Nachweis auf eine Fundstelle des Gesetzgebers.
[570] Pankoke, Von der Presse- zur Providerhaftung, S. 38, der allerdings seine Ausführungen noch zu § 5 Abs. 3 TDG a.F. gemacht hat. Da jedoch die Problematik der „Zugangsvermittlung" im Mittelpunkt steht, müssen seine Anmerkungen für die neuen Haftungsregelungen des TDG (§§ 9 ff. TDG) entsprechend gelten (vgl. auch Köhler/Arndt/Fetzer, Recht des Internet, S. 257). Vgl. ebenso Pankoke, Von der Presse- zur Providerhaftung, S. 45 mit dem Hinweis, dass die Formulierung des § 2 Abs. 4 Nr. 1 TDG aus dem Grunde missglückt sei, da sämtliche inhaltsbezogenen Teledienste zugleich auch Telekommunikationsdienstleistungen sind und das TDG daher praktisch nie zur Anwendung käme. Daher erscheine rechtspolitisch nur eine parallele Anwendung sinnvoll.
[571] Vgl. auch Tettenborn, MMR 1999, 516, 518, der ebenfalls auf eine grundsätzliche Trennung zwischen Transport- und Inhaltsebene verweist.

auf einer Telekommunikationsdienstleistung basiert, was bereits durch § 2 Abs. 1 TDG („mittels Telekommunikation“) so vorgesehen ist, sind die einzelnen Dienste funktional zu trennen und auf jedes Angebot das entsprechende Gesetz anzuwenden.[572] Dementsprechend bleibt der Anwendungsbereich der §§ 9 ff. TDG für diejenigen Provider erhalten, die inhaltliche Dienstleistungen unter (zwangsläufiger) Nutzung der Transportebene des Internet erbringen. Dies bedeutet, dass die Anwendung der funktionalen Betrachtungsweise für die Beurteilung einer „Einzel“-Leistung eines kombinierten Online-Dienstes (weiterhin) erforderlich ist.[573]

Zum anderen ist bei richtigem Verständnis der Anbieter eines Telekommunikationsdienstes ebenso wenig, d.h. auch ohne Haftungsprivilegierung der §§ 9 ff. TDG, im Sinne der allgemeinen Vorschriften des BGB haftbar, wenn er keinen inhaltlichen Einfluss auf die versendeten Informationen hatte, deren Transport er übernimmt.

Nach § 9 TDG tragen Dienstleister, die fremde Informationen lediglich übermitteln oder den Zugang zu diesen vermitteln, keine Verantwortung[574] für diese.[575] Eine solche Sichtweise muss gleichermaßen im Rahmen der allgemeinen Haftungsmaßstäbe gelten.[576]

---

[572] Vgl. die Ausführungen auf S. 66 ff.

[573] Siehe zur dienstorientierten Betrachtungsweise die Ausführungen auf S. 74.

[574] Unter Verantwortlichkeit im Sinne der Haftungsprivilegierung ist dabei das Einstehenmüssen des Diensteanbieters für Rechtsverletzungen, gleichgültig aus welchem Rechtsgebiet sie stammen, zu verstehen, vgl. Spindler, MMR 1998, 639, 640; Freytag, ZUM 1999, 185, 190;; siehe zum Begriff der Verantwortlichkeit auch Koch, CR 1997, 193, 196.

[575] Vgl. auch LG München, CR 2000, 117, 119, welches die Regelung des § 5 Abs. 3 TDG a.F. unter der Schuldfrage berücksichtigt. Nach anderer Auffassung soll die Haftungsprivilegierung als eine Art zusätzlicher Filter vor den allgemeinen Vorschriften geprüft werden, vgl. Vassilaki, MMR 1998, 630, 636 ff.; Bleisteiner, Rechtliche Verantwortung im Internet, S. 157; Beucher/Leyendecker/v. Rosenberg, Mediengesetze-Kommentar, § 5 TDG Rn. 2/28; Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2984; Gounalakis/Rhode, Persönlichkeitsschutz im Internet, Rn. 291/292/295. Siehe im Besonderen Freytag, Haftung im Netz, S. 209 ff., der die Verantwortlichkeit im Sinne von § 5 TDG a.F. nach der objektiven Rechtsverletzung und Kausalität und vor der Frage der Rechtswidrigkeit und Schuld prüft, aber darauf hinweist (S. 217), dass keine Wertungswidersprüche entstehen dürfen. Freytag (aaO) führt aus, dass im Falle einer Bejahung der Vorhersehbarkeit und Vermeidbarkeit der Rechtsverletzung (im Rahmen der vorgelagerten Verantwortlichkeit von § 5 TDG a.F.) diese daher auch bei der Verschuldensprüfung bejaht werden müssen, wobei darüber hinausgehend ein Verschulden auch aufgrund der konkreten Umstände des Einzelfalls entfallen kann, und zwar selbst wenn die Voraussetzungen des § 5 TDG a.F. verneint wurden.

[576] Siehe hierzu etwa Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 36 ff./89 ff. sowie S. 117/118 mit dem Hinweis, dass Access-Provider zivil- und strafrechtlich nur eingeschränkt verantwortlich sind. Danach sind Access-Provider aus positivem Tun nach deutschem Strafrecht nur dann verantwortlich, wenn ihnen wegen inhaltlicher Gestaltung (wenn der Access-Provider gleichzeitig Content-Provider ist) oder Kenntnis vom Inhalt der Daten ein positives Tun vorgeworfen werden kann (siehe Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet,

Sowohl Telekommunikationsanbieter als auch Zugangsvermittler übertragen technische Signale, auf deren Inhalt sie keinen Einfluss haben.[577] Der Access-Provider kann die Informationen, die über das Netz transportiert werden, nicht „prophezeien“, so dass er haftungsrechtlich nicht dafür einstehen kann. Die Informationen liegen außerhalb seines Verantwortungsbereichs.

Insofern ist in § 9 TDG nur das gesetzlich fixiert, was allgemein im Rahmen der Bewertung der Schuldfrage oder Verantwortlichkeit eines Access-Providers ohnehin gelten muss, wenn es um seine Haftung für fremde Inhalte bzw. Informationen geht:
Hat ein Access-Provider keinen Einfluss auf die Gestaltung von (rechtswidrigen) Informationen hat, so handelt er bei deren Weitertransport und allein durch die Bereitstellung der Kommunikationsvoraussetzungen weder vorsätzlich[578] noch fahrlässig.[579] Er ist daher zivil- und strafrechtlich nur eingeschränkt verantwortlich,[580] und er verletzt keine Sorgfaltspflichten, wenn er die Informationen nicht überwacht.[581]

S. 117/118). Bei einem Unterlassen (wenn der Access-Provider nur den Internetzugang verschafft) scheidet hingegen eine Strafbarkeit aus, wobei das gleiche für die zivilrechtlichen Ansprüche auf Schadensersatz gilt, die in ihrer sanktionierenden Wirkung nicht über das Maß der strafrechtlichen Normen hinausgehen (Herzog aaO).

[577] Vgl. Riehmer/Hessler in: Spindler, Vertragsrecht der Internet Provider (1. Auflage), Teil II Rn. 175. Ausnahmen von der Verantwortlichkeit sollen dann greuifen, wenn die Tätikeit des Diensteanbieters auf den technischen Vorgang beschränkt ist, ein Kommunikationsnetz zu betreiben und den Zugang zu diesem zu vermitteln (vgl. Stögmüller in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 188.

[578] Vorsatz ist das Wissen und Wollen der objektiven Tatbestandsmerkmale (siehe hierzu anstatt vieler Grundmann in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, § 276 BGB Rn. 155 ff.; derselbe in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2a, Rn. 155 ff.).

[579] Fahrlässigkeit bedeutet gemäß § 276 Abs. 1 S. 2 BGB die Nichtbeachtung der im Verkehr erforderlichen Sorgfalt (siehe anstatt vieler Grundmann in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, § 276 BGB Rn. 50; derselbe in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2a, Rn. 50).

[580] Vgl. Herzog aaO (Fn. 576).

[581] Vgl. BGH MMR 2004, S. 166 ff. insbesondere mit der Begründung, dass es dem Betroffenen als Anspruchsteller weder unzumutbar noch unmöglich ist nachzuweisen, dass er den Internet-Provider konkret auf einen von ihm bereitgehaltenen rechtswidrigen fremden Inhalt in seinem Internetangebot hingewiesen hat. Wenn er ein konkretes Angebot auf den Servern des Providers benennt und beschreibt, indem er etwa den Aufbau, die wesentlichen Text- und Bildbestandteile und den Dateinamen einer Website auf dem Server mitteilt und gegebenenfalls einen entsprechenden Ausdruck beifügt, wird der Beweis dieses Hinweises in aller Regel als Beweis für die Kenntnis des Providers ausreichen, wenn dieser hiermit die fraglichen Inhalte ohne unzumutbaren Aufwand auffinden kann. Siehe hierzu auch Spindler, MMR 2004, S. 440 ff. Vgl. außerdem Kloepfer, Informationsrecht, § 13 Rn. 43, der darauf verweist, dass Access-Provider nicht verpflichtet sind, Inhalte, zu denen sie den Zugang vermitteln, fortlaufend auf ihre Rechtmäßigkeit zu kontrollieren. Ebenso Sieber, ZUM 1999, 196, 196, der unabhängig von der Frage, ob Access-Providing als Teledienst einzuordnen ist und die Haftungsprivilegierung des TDG fällt, feststellt, dass Network- und Access-Providern eine Kontrolle und Sperrung der im

Hiervon unberührt bleibt die Verpflichtung zur Entfernung oder Sperrung von Informationen ab Kenntniserlangung, wie sie auch in § 8 Abs. 2 TDG normiert ist.[582]

Bei der Prüfung der Schuldfrage wird dementsprechend der Access-Provider nicht unbillig benachteiligt, sofern nach richtigem Verständnis im Rahmen der allgemeinen zivilrechtlichen Verantwortung die gleichen Maßstäbe angelegt werden wie im Rahmen von § 5 Abs. 3 TDG a.F. bzw. § 9 TDG.[583]
In rechtspolitischer Hinsicht kann die Überlegung angestellt werden, ob § 2 Abs. 4 Nr. 1 TDG zu ergänzen ist, so dass die Haftungsprivilegierungen der §§ 9 ff. TDG für Telekommunikationsdienstleistungen entsprechende Geltung erlangen.[584]
Vom Sinn und Zweck der Regelung gemäß § 9 TDG wäre dies passend,[585] da es sich hier ebenso um eine Tätigkeit technischer, automatischer und passiver Art handelt, bei der der Diensteanbieter in keiner Weise mit der übermittelten Information in Verbindung steht.
Im Sinne der Gesetzessystematik und unter Berücksichtigung, dass das TKG für Telekommunikationsdienste und das TDG für Teledienste gilt, wäre eine solche klarstellende Haftungsprivilegierung für Telekommunikationsdienste aber allenfalls im TKG und nicht im TDG angebracht. Folgt man der obigen Argumentation kann darauf jedoch ebenso verzichtet werden.

Internet übermittelten Inhalte im Internet grundsätzlich nicht möglich ist. Er ist der Ansicht, dass eine Kontrolle aufgrund der großen Datenvolumina technisch nicht möglich und außerdem rechtspolitisch nicht wünschenswert ist, da dies im Sinne eines effektiven Schutzes nur zu einem Verschlüsselungsverbot führen kann.
[582] Vgl. Stögmüller in: Spindler, Vertragsrecht der Internet Provider, Teil II Rn. 185/192.
[583] Köhler/Arndt/Fetzer, Recht des Internet, S. 257 weisen darauf hin, dass § 5 Abs. 3 TDG a.F. durch § 9 TDG ersetzt worden ist bzw. die bisherige Regelung des § 5 Abs. 3 TDG a.F. dahingehend präzisiert, dass ein Diensteanbieter nur dann für fremden Content verantwortlich ist, wenn er den Content auch lediglich in einem Kommunikationsnetz übermittelt oder den Zugang zur Nutzung des Content vermittelt.
[584] Pankoke, Von der Presse- zur Providerhaftung, S. 45 schlägt eine Streichung von § 2 Abs. 4 Nr. 1 TDG und Ergänzung von Abs. 5 dahingehend vor, dass die Vorschriften des TKG unberührt bleiben.
[585] Anmerkung Schütz/Attendorn zu LG Frankenthal, MMR 2001, 401, 405.

ddd. Abgrenzung am Beispiel von Suchmaschinen[586]

Access-Providing ist insbesondere aus dem Grunde nicht als Teledienst einzustufen und unter § 2 Abs. 2 Nr. TDG zu subsumieren, da nach dem Wortlaut dieser Norm andere Sachverhalte geregelt werden.
So fallen unter § 2 Abs. 2 Nr. 3 TDG beispielsweise Navigationshilfen[587] oder Suchmaschinen.[588]
Bei Suchmaschinen werden dem Nutzer sowohl fremde Inhalte bzw. Informationen im Sinne von § 3 Nr. 1 2. Alt TDG durch Verlinkung[589] vermittelt, als auch für den Nutzer eigene Inhalte des Suchmaschinenbetreibers im Sinne von § 3 Nr. 1 1. Alt., § 2 Abs. 2 Nr. 3 TDG bereitgehalten. [590] Letzteres bezieht sich auf die Art und Weise der Gestaltung der „Suchmaschinen-Website" (beispielsweise Impressum, Werbebanner) und die Auflistung der Suchergebnisse,[591] womit es sich um eigene Informationen handelt.[592]

---

[586] Siehe hierzu etwa die Suchmaschinen www.google.de, www.altavista.de, www.metager.de (anstatt vieler anderer).
[587] Siehe „Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)", Bundestag-Drucksache 13/7385, S. 19 (nachfolgend: Bundestag-Drucksache 13/7385).
[588] Eine Suchmaschine ist ein spezieller Server im Internet, der Datenbanken über zahlreiche im Internet öffentlich zugängliche Informationen (insbesondere WWW-Seiten) führt (siehe Sieber in: Hoeren/Sieber, Teil 1 Rn. 99 ff.). Zur Funktionsweise der Suchmaschinen siehe auch Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 52 ff. Siehe zu Suchmaschinen ebenso Brühann in: Gounalakis, Rechtshandbuch Electronic Business, § 8 Rn. 41 mit dem Hinweis, dass Suchmaschinen die Technik der Indexerstellung durch Stichwörter verwenden.
[589] Verweise bzw. Verknüpfungen auf andere Textstellen, Medien oder Dokumente werden als Hyperlink oder kurz Link bezeichnet. Mit ihrer Hilfe kann man innerhalb eines Dokuments oder zwischen verschiedenen Dokumenten Vernetzungen aufbauen. Ein Link wird durch Anklicken mit der Maus aktiviert und ruft die verbundene Textstelle bzw. ein anderes Dokument auf (Voss, Das große PC & Internet Lexikon 2007, „Hyperlink" S. 426. Siehe auch Kloepfer, Informationsrecht, § 13 Rn. 29, der darlegt, dass Suchmaschinen wie Yahoo, Altavista, Lycos oder Google, nach Eingabe von Suchbegriffen durch den Nutzer Listen von Fundstellen zusammenstellen, so dass der Nutzer auf diese fremden Tele- oder Mediendienste durch Anklicken der Hyperlinks Zugriff nehmen kann.
[590] Oben wurde bereits dargestellt, dass sich die Differenzierung zwischen Zugangsvermittlung (§ 3 Nr. 1 2. Alt. TDG) und dem Bereithalten von Angeboten zur Nutzung von Diensten (§ 2 Abs. 2 Nr. 3 TDG, § 3 Nr. 1 1. Alt. TDG) eindeutig aus dem Gesetz ergibt (siehe oben Fn. 563 mit dem Verweis auf die Ausführungen von Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 78. Vgl. auch Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 87 Fn. 459).
[591] Vgl. auch Waldenberger in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDG Rn. 25. Im Rahmen dieser Ausführungen soll im Übrigen lediglich dargestellt werden, dass der Anbieter einer Suchmaschine, die (Auflistung der) Suchergebnisse auf einem eigenen Server bereithält und damit ein eigenes inhaltliches Angebot ins Netz stellt. Davon zu unterscheiden ist aber die Frage, inwieweit er für die Inhalte, auf die er verweist, zivil- und strafrechtlich zur Verantwortung gezogen werden kann. Siehe auch Sieber in: Hoeren/Sieber, Teil 19 Rn. 275, der darauf verweist, dass die von den Suchmaschinen *ausgewiesenen* Inhalte keine „bereitgehaltenen" Daten im Sinne von § 5 Abs. 2 TDG a.F. sind, sondern dass Suchmaschinen vielmehr den Zugang zu fremden Inhalten vermitteln.

Betreiber von Suchmaschinen nehmen dementsprechend ein Doppelfunktion ein, indem sie zum einen durch ihre eigenen Angebote, sprich ihrer eigenen Website, die das Angebot zum Suchen und zur Nutzung des Internet enthält, Telediensteanbieter im Sinne von § 2 Abs. 2 Nr. 3 TDG sind.
Zum anderen fallen sie jedoch darüber hinaus ebenso unter den Begriff der Zugangsvermittler im Sinne von § 3 Nr. 1 2. Alt. TDG, da sie fremde Inhalte bzw. Informationen nicht etwa auf ihren Servern bereithalten, sondern lediglich durch entsprechende technische Gestaltung im Sinne von Links den Zugang hierzu vermitteln.[593]

---

[592] Die Suchmaschine „Yahoo" listet gegen entsprechendes Entgelt von Anzeigenkunden auf ihrer Website beispielsweise sowohl Links von Sponsoren als auch getrennt davon „sponsorenfreie" Links als „Top 20 Web-Sites" (als eigenes Angebot) auf.

[593] Im Sinne der Gesetzesbegründung (siehe Bundestag-Drucksache 13/7385, S. 20, wonach Zugangsvermittlung und die Nichtverantwortlichkeit für Inhalte im Sinne von § 5 Abs. 3 TDG a.F. vorliegen soll, wenn Diensteanbieter zu fremden Inhalten lediglich den Weg öffnen) fallen auch Suchmaschinen unter die Zugangsvermittlung (vgl. auch Sieber in: Hoeren/Sieber, Teil 19 Rn. 275, der eine Zugangsvermittlung für Betreiber von Suchmaschinen bejaht, da diese die fremden Inhalte nicht beherrschen; vgl. auch Fn. 560, wonach für das Bereithalten auch ein Beherrschen über die Daten erforderlich ist. Ein Beherrschen ist lediglich in Bezug auf die Art und Weise der Gestaltung der Website des Suchmaschinenbetreibers, etwa im Hinblick auf die Werbung, der Fall, aber nicht im Hinblick auf die Daten, die „hinter" den Suchergebnissen stehen.). Zu trennen ist daher bei Suchmaschinen zwischen dem eigenen Angebot auf der Website des Suchmaschinenbetreibers und den fremden Inhalten, zu denen die Suchmaschinenbetreiber den Zugang vermitteln, und für die sie gegebenenfalls gemäß § 9 TDG von der Haftung befreit sein können. Diese Haftungsbefreiung soll in dieser Arbeit jedoch nicht vertieft behandelt werden, da dies außerhalb des Betrachtungsgegenstandes liegt und der Rahmen dieser Arbeit dadurch ausufern würde (vgl. hierzu auch Koch, CR 2004, 213, 214 ff., der die Anwendbarkeit von §§ 9 – 11 TDG auf Suchmaschinen und Links ablehnt; siehe außerdem Schwarz in: Gounalakis, Rechtshandbuch, Electronic Business, § 54 Rn. 135 ff. zu Links sowie Rn. 140 ff. zur Haftung der Suchmaschinenbetreiber. Schwarz (aaO) lehnt die Anwendbarkeit von § 11 TDG auf Suchmaschinenbetreiber mit dem Argument ab, dass es nicht der Suchmaschinenbetreiber, sondern ein anderer Diensteanbieter sei, der die die Inhalte bereitstelle. Siehe zur Anwendbarkeit von § 11 TDG auf Suchmaschinenbetreiber auch LG Frankenthal, CR 2006, S. 698, 699, welches in dem zu entscheidenden konkreten Sachverhalt jedoch von einem Mediendienst ausgegangen ist). Zur weiteren Information wird auf die nachfolgenden Fundstellen verwiesen: So wird die Funktion der Zugangsvermittlung mit der Begründung anerkannt, dass Zugangsvermittlung nicht mit Access-Providing gleichzusetzen ist und nicht nur das Eröffnen des nutzerseitigen Zugangs zum Internet erfasst, sondern vielmehr auch sonstige Formen des Zugänglichmachens von Inhalten (so Koch, CR 1997, 193, 200; vgl. hierzu auch Spindler in: Roßnagel, Recht der Multimedia-Dienste, § 5 TDG Rn 113 ff.; Sieber, MMR-Beilage 2/1999, 1, 22; Wimmer, ZUM 1999, 436, 440; Spindler, NJW 1997, 3193, 3198. Siehe aber ebenso v.Bonin/Köster, ZUM 1997, 821, 825, die eine Zugangsvermittlung nur für diejenigen bejahen wollen, die mit „den Inhalten nichts zu tun haben"; ähnlich auch Freytag, ZUM 1999, 185, 192, der eine Zugangsvermittlung nur für die Fälle anerkennt, bei denen bereits aufgrund feststehender technischer Parameter ein inhaltlicher Bezug des Anbieters zu den übermittelten Informationen ausscheidet. Sieber (vgl. Sieber in: Hoeren/Sieber, Teil 19 Rn. 275/284) versteht zwar einerseits die Zugangsvermittlung rein technisch, aber sieht darin andererseits keinen Widerspruch, die Suchmaschine dennoch als Zugangsvermittlung einzuordnen, wie sich aus seinen Ausführungen ergibt. Diese Ansicht ist auch überzeugend, da die Gesetzesbegründung zu § 5 Abs. 3 TDG a.F. (der wie oben bereits ausgeführt durch § 9 TDG ersetzt worden ist) diejenigen Funktionen von der Haftung ausnehmen will, die einem reinen Telekommunikationsdienst vergleichbar sind (siehe Bundestag-Drucksache 13/7385, S. 19), so dass im Rahmen der Verlinkung bei der Suchmaschine geprüft werden muss, inwieweit

Hier ist folglich der Unterschied zum Access-Provider begründet.
Der Access-Provider hält keine eigenen oder fremden Inhalte zur Nutzung bereit, sondern vermittelt den Zugang zu diesen Inhalten. Hierbei handelt es sich um eine rein technische Zugangsvermittlung, wobei der Unterschied zum Suchmaschinenbetreiber darin liegt, dass er für den Vorgang der Zugangsvermittlung zu fremden Informationen keine eigene Website bzw. keine eigenen inhaltlichen Angebote unterhält,[594] über welche ein Nutzer notwendigerweise und nur über diese zu anderen Inhalten gelangt. Ein Access-Provider stellt vielmehr die technischen Voraussetzungen[595] für den Zugang zur Verfügung.
Beim Access-Providing muss der Nutzer nicht auf ein inhaltliches Angebot zugreifen, um von dort anschließend weitergeleitet zu werden. Hier ist vielmehr allein ein technischer Vorgang (der Vermittlung) erforderlich, ohne den „Umweg" über ein inhaltliches Angebot des Access-Providers gehen zu müssen.[596]
Zu berücksichtigen ist hier, dass das Telekommunikationsrecht den Transport der Daten betrifft, währenddessen sich das Recht im Zusammenhang mit den Telediensten auf die Nutzung des Internets zwecks Befriedigung der Informations- und Konsumbedürfnisse der Nutzer bezieht.[597]
Access-Providing erfüllt daher insgesamt eine andere Funktion als eine Suchmaschine.[598]

---

derjenige, der den Link setzt, „mit den Inhalten etwas zu tun hat" (siehe oben v.Bonin/Köster aaO) oder aber ein inhaltlicher Bezug ausscheiden muss (siehe oben Freytag aaO), weil der Link im Sinne der Gesetzesbegründung eher eine technische Funktion im Sinne eines Telekommunikationsdienstes einnimmt. Letzteres ist bei Suchmaschinen stets der Fall, da hier weder ein „qualifizierter" Link noch ein „Zu-eigen-machen" vorliegt (siehe hierzu Fn. 599).

[594] Siehe Fn. 562 in dieser Arbeit sowie den dortigen Verweis auf Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 87 Fn. 459, der zu Recht auf die Notwendigkeit einer solchen Website hinweist.

[595] Diese technischen Voraussetzungen werden durch die Bereitstellung eines PoP geschaffen, siehe S. 122 ff.

[596] Siehe auch S. 32.

[597] Vgl. Gola/Klug, Gründzüge des Datenschutzrechts, S. 187. Auch diese Definition zeigt im Übrigen, dass es angebracht sein könnte, bei der Bereitstellung einer Suchmaschine einen einheitlichen Teledienst zugrunde zu legen (ohne Trennung zwischen Website und Link), da der Nutzer einer solchen vorrangig seine Informationsbedürfnisse befriedigen möchte, wohingegen er beim Internetzugang seine Daten(anfrage) transportiert wissen möchte.

[598] Suchmaschinen, wie etwa yahoo, werden teilweise mit Suchdiensten, wie Archie oder Gopher, gleichgesetzt (vgl. zu diesen Begriffen Hobert, Datenschutz und Datensicherheit im Internet, S. 46/47; Cichon, Internetverträge (1. Auflage), S. 10; teia (Hrsg.), Recht im Internet, S. 39, die darauf verweisen, dass es sich hierbei um veraltete Dienste handelt, die mittlerweile kaum noch von Bedeutung sind; zur Definition siehe außerdem Koch, Internet-Recht, S. 562/563 (so noch in der 1. Auflage)) und als Internet-Dienste eingeordnet (siehe etwa Kröger/Göers/Hanken, Internet für Juristen, S. 21 ff.; Kröger/Kuner, Internet für Juristen, S. 16

Darüber hinaus könnte allenfalls für einen Suchmaschinenbetreiber fraglich sein, ob zwischen der Website des Suchmaschinenbetreibers (§ 2 Abs. 2 Nr. 3 TDG) sowie dem Link als Zugangsvermittlung (§ 3 Nr. 1 2. Alt. TDG) zu trennen ist. Damit einher geht die Frage, ob dieser Link der Suchmaschine gegebenenfalls als Telekommunikationsdienst nach § 3 Nr. 24 TKG eingestuft werden könnte, so dass aufgrund der Regelung in § 2 Abs. 4 TDG das Teledienstegesetz und somit § 3 Nr. 1 2. Alt. TDG für die Verlinkung erst gar nicht in Betracht kommt.

Eine vertiefende Auseinandersetzung mit der Haftungsprivilegierung bei Links wäre allerdings zum einen wegen der vielfältigen Meinungen zu dieser Rechtsfrage zu umfassend.[599] Zum anderen würde es die hier aufgeworfene

---

ff.; Sieber in: Hoeren/Sieber, Teil 1 Rn. 99 ff.). Im Sinne der oben entwickelten Definition (S. 75 ff.) ist aber zu beachten, dass Internet-Dienste wie beispielsweise Archie und Gopher technische Werkzeuge bzw. Internet-Funktionen zur Datenverarbeitung und Datendarstellung darstellen, denen entweder spezielle Protokolle oder Programmsysteme zugrunde liegen, und die aufgrund dieser technischen Voraussetzungen bzw. Möglichkeiten eine weltweite Datenübertragung ermöglichen (vgl. Sieber in: Hoeren/Sieber, Teil 1 Rn. 79; Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 26; zum Gopher-Protokoll siehe außerdem noch Voss, Das große PC-Lexikon, S. 849 (1. Auflage - in der aktuellen Auflage „Das große PC & Internet Lexikon 2007“ ist zu diesem Protokoll keine Begriffserklärung mehr enthalten), und Tanenbaum, Computernetzwerke, S. 678; zu gopher, WAIS und Archie siehe auch Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 13; vgl. zum Such- und Internet-Dienst WAIS –Wide Area Information Server ebenso Hobert, Datenschutz und Datensicherheit im Internet S. 47). Daher sollte der jeweilige Suchservice, sprich Suchmaschinen wie google, yahoo, altavista, etc. nicht als Internet-Dienst bezeichnet werden, sondern allenfalls die den Suchmaschinen zugrunde liegende Technik (in der Regel das WWW mit seinem speziellen http-Protokoll oder auch ftp-Protokoll, siehe hierzu etwa: Sieber in: Hoeren/Sieber, Teil 1 Rn. 131/132; teia (Hrsg.), Recht im Internet, S. 34/39; Kröger/Göers/Hanken, Internet für Juristen, S. 24). Der Service an sich bzw. die angebotene Suchmaschine sollte dann im Sinne der obigen Ausführungen als Teledienst eingeordnet werden. Siehe aber auch Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I Rn. 51, der Suchmaschinen eine besondere Einflussnahme auf die Meinungsbildung unterstellt und sie daher als Mediendienste gemäß § 2 Abs. 2 Nr. 4 MDStV einordnet.

[599] Bei Links ist (ebenso wie bei Suchmaschinen, siehe Fn. 593) grundsätzlich umstritten, inwieweit die Haftungsprivilegierungen des TDG greifen. Da auch hier eine vertiefte Behandlung außerhalb des Betrachtungsgegenstandes liegt, und der Rahmen der Arbeit ausufern würde, wird an dieser Stelle zur weiteren Information zumindest auf die nachfolgenden Fundstellennachweise verwiesen: Winteler in: Moritz, Rechts-Handbuch zum E-Commerce, B Rn. 500; Koch, CR 2004, S. 213, 215; Siehe ebenso Gounalakis/Rhode, Persönlichkeitsschutz im Internet, Rn. 303, die eine Anwendbarkeit von § 11 TDG für Links bejahen. Vgl. zu § 5 TDG a.F. Bettinger/Freytag, CR 1998, 545, 549; Spindler, NJW 1997, 3193, 3198; Beucher/Leyendecker/v. Rosenberg, Mediengesetze-Kommentar, § 5 TDG Rn. 35; Waldenberger, AfP 1998, 373, 374; Waldenberger, MMR 1998, 124, 128 ff.; Altenhain, AfP 1998, 457, 464; Kloepfer, Informationsrecht, § 13 Rn. 46 ff., der zwischen drei Arten von Links unterscheidet, und eine Haftungsfreistellung nach § 5 Abs. 3 TDG a.F. nur in Betracht kommen soll, wenn weder eine redaktionelle Bezugnahme noch nähere Erläuterungen auf weiterführende Angebote hinweisen; bei „qualifizierten“ Links hingegen, die gerade im Bewusstsein des fremden Inhalts eingerichtet werden oder bei denen gar ein Vereinnahmungswille der Inhalte vorliegt, soll eine Haftung nach § 5 Abs. 2 TDG a.F. oder § 5 Abs. 1 TDG a.F. in Betracht kommen. Siehe hierzu auch Spindler, NJW 1997, 3193, 3198. Siehe außerdem Freytag, Haftung im Netz, S. 228 ff., der sich für die generelle Anwendbarkeit von § 5 Abs. 2 TDG a.F. ausspricht. Zu §§ 8 ff. TDG und der Frage der Verantwortlichkeit für

Problematik, ob es sich bei der Dienstleistung des Access-Providing um einen Teledienst handelt, nicht wesentlich voranbringen. Zur Beantwortung dieser Frage reicht die oben getroffene Feststellung aus, dass Access-Providing insgesamt eine andere Funktion als eine Suchmaschine im Sinne des § 2 Abs. 2 Nr. 3 TDG erfüllt und damit von dieser Norm nicht erfasst wird.
Daher sei an dieser Stelle lediglich auf die Fundstellennachweise in der vorherigen Fußnote verwiesen. Ergänzend soll angemerkt werden, dass es angebracht erscheint, von einem einheitlichen Teledienst auszugehen, da Suchmaschinen notwendigerweise Links enthalten und eine Suchmaschine ohne Verlinkung ihre Funktion nicht erfüllen könnte.[600] Insbesondere geht auch der Gesetzgeber bei einer Suchmaschine insgesamt von einem Teledienst aus.[601]

cc. Fazit: „Access-Providing als Telekommunikationsdienst“

Bei Access-Providing handelt es sich um einen Telekommunikationsdienst im Sinne von § 3 Nr. 24 TKG sowie um einen Online-Dienst, da es sich um wirtschaftliche Tätigkeiten handelt, die im Internet erbracht werden bzw. in der Vermittlung zum Internet bestehen.[602]
Bei der Einordnung der Leistung des Access-Providers als Telekommunikationsdienst ist es im Übrigen nicht von Bedeutung, ob bei einem Internetzugang die W-Lan-Technik eingesetzt wird, da ein W-Lan lediglich eine drahtlose „verlängerte“ Verbindung zwischen Rechnern und

---

Hyperlinks siehe LG Frankenthal, MMR 2001, 401 ff.; siehe ebenso hierzu Anmerkung Schütz/Attendorn zu LG Frankenthal, MMR 2001, 401, 405).

[600] Etwas anderes kann allenfalls für Links gelten, die auf „herkömmlichen“ Websites gesetzt sind. Hier haben die Websites regelmäßig nicht vorrangig die Funktion der Zugangsvermittlung zu anderen Websites bzw. Angeboten, auch wenn sie Links enthalten, sondern dienen dazu, eigene Informationen darzustellen. Daher könnten die auf dieser Website enthaltenen Links durchaus unabhängig bzw. als eigenständiger Dienst/Angebot zu bewerten sein, was in dieser Arbeit jedoch nicht näher untersucht werden kann. Ansatzpunkt könnte aber sein, ob es sich um einen „qualifizierten“ Link handelt oder ob ein „Zu-Eigen-machen“ der fremden Information in Betracht kommt (siehe vorherige Fn. 599), so dass der Link unter § 3 Nr. 1 1. Alt. TDG als Bereithalten von Informationen fällt. Sofern dies nicht der Fall steht, dürfte regelmäßig der Übertragungs- bzw. Weiterleitungsvorgang als rein technischer Vorgang im Vordergrund stehen, so dass es sich um einen Telekommunikationsdienst nach § 3 Nr. 24 TKG handelt. Entsprechend der Ausführungen beim Access-Providing wäre daher nicht § 9 TDG anwendbar, sondern es müsste im Rahmen der allgemeinen Schuldfrage geprüft werden, inwieweit eine Verantwortung desjenigen, der den Link gesetzt hat, in Betracht kommen kann (vgl. hierzu S. 131 ff.). Siehe zur Regelungslücke von Suchmaschinen und Links auch Koch, CR 2004, 213, 214 ff.

[601] Siehe Bundestag-Drucksache 13/7385, S. 19.

[602] Siehe zur Begriffsdefinition des Online-Dienstes S. 71.

Teilnehmeranschlussdose darstellt. Es soll mittels eines W-Lan die Verbindung überbrückt werden, die mittels Leitungen nicht praktikabel durchführbar ist. Damit werden aber lediglich Daten von einem im Büroraum stehenden Rechner („Bluetooth“) zu der nächsten (Anschluss)Dose drahtlos übertragen oder Rechner in einem Gebäude drahtlos vernetzt.[603]

b. Notwendige Infrastruktur

Oben wurde dargestellt, dass eine Internetverbindung nicht nur aus der Dienstleistung des Access-Providing besteht, sondern mehrere Dienstleistungen umfasst.[604] Hierzu gehört ebenso die Bereitstellung der notwendigen (Telefon)Leitungen (nachfolgend: TK-Providing) sowie DNS und Routing ,[605] die im Folgenden einer rechtlichen Betrachtung unterzogen werden. Im Sinne der Begriffsdefinition „Online-Dienst“ in dieser Arbeit handelt es sich bei TK-Providing, DNS-Service und Routing gleichermaßen um Online-Dienste, da es wirtschaftliche Tätigkeiten darstellen, die im Internet erbracht werden oder in der Vermittlung zum Internet bestehen. TK-Providing steht zwar nicht zwangsläufig mit dem Internet in unmittelbarem Zusammenhang, da mittels TK-Providing ebenso der Telefon- oder Faxverkehr abgewickelt werden kann. Da aber TK-Providing zumindest eine Teilleistung des Online-Dienstes VPN darstellt und regelmäßig notwendig ist, um den Zugang ins Internet zu

[603] Siehe zur technischen Verbesserung der W-Lan-Technik „Wimax“ aber auch Fn. 125. Vgl. auch Röhrborn/Katko, CR 2002, 882, 882/883, die anmerken, dass mit Hilfe von Basisstationen, die derzeit über 500 Meter Reichweite haben, Privathäuser und Bürogebäude drahtlos vernetzt werden, insbesondere auch um die nachträgliche Verkabelung von älteren Bürogebäuden verzichtbar zu machen. Siehe auch Horns in: Abel, Datenschutz in Anwaltschaft, Notariat und Justiz, § 14 Rn. 55 ff., der im Zusammenhang mit der W-Lan-Technik auf den Datenübertragungsstandard „Bluetooth“ zur Funkübertragung im Nahbereich verweist, mit dem kabellos die schnelle und kostengünstige Übertragung von Daten in kleinen, sich selbst organisierenden Netzwerken erreicht werden soll. Hierbei verweist er auch auf mögliche Verschlüsselungsmechanismen (Rn. 58). Zur „Bluetooth“-Technik siehe auch Tanenbaum, Computernetzwerke, S. 37, 345 ff.

[604] Siehe S. 121.

[605] Köhntopp/Köhntopp, CR 2000, 248, 249. Siehe zur Darstellung des DNS S. 30. Im Folgenden werden die Anbieter von Routing und DNS als Routerbetreiber bzw. DNS-Server-Betreiber bezeichnet. Vgl. auch Bundestag-Drucksache 14/1191, S. 7: Für den Nutzer wird die Möglichkeit, im Internet zu surfen, nicht bereits durch den Aufbau einer ständigen Verbindung über die Telefonleitung zum Provider hergestellt. Voraussetzung sind vielmehr neben der Einwahlmöglichkeit auch die zum Verbindungsaufbau notwendigen Protokollfunktionen und die Vergabe der IP-Adresse,
(Domain-)Name-Service und Routing. Access-Provider erbringen regelmäßig auch den DNS-Dienst (vgl. OLG Hamburg, MMR 2000, 278 ff.; Schaar, Datenschutz im Internet, Rn. 23, Rn. 262).

vermitteln, ist insoweit eine Einstufung als Online-Dienst gerechtfertigt. Dies wird im nachfolgenden Punkt nochmals verdeutlicht.

aa. TK-Providing

Ohne die Anbieter Telekommunikationsnetzen, im folgenden TK-Provider, ist der Internetzugang nicht möglich.[606] Hierbei muss es sich jedoch nicht zwangsläufig um Festnetzprovider handeln,[607] da gleichermaßen das Handy eine Kommunikationszentrale[608] darstellen kann.[609]

TK-Provider sind Anbieter eines Telekommunikationsdienstes nach § 3 Nr. 24 TKG. Denn hier wird durch die Bereitstellung der entsprechenden netztechnischen Infrastruktur den Nutzern allein die Möglichkeit zur Verfügung gestellt, Daten zu übertragen. Diese Bereitstellung erfolgt anwendungsdiensteunabhängig.[610]

bb. DNS-Service

DNS[611] gehört zur notwendigen Internet-spezifischen Infrastruktur.[612]

Der DNS-Server wird von Access-Providern oder anderen Providern betrieben, um den Verbindungsaufbau zu gewährleisten. Damit liegt der Schwerpunkt der Leistung auf der Verständigungsmöglichkeit zwischen Sender und Empfänger, da ohne DNS-Server die entsprechenden Domains nicht ohne weiteres auffindbar wären und der Kommunikationsvorgang unerträglich erschwert, wenn nicht sogar unmöglich gemacht werden würde. Dies gilt gleichermaßen für das dynamische DNS-Verfahren, wo eine Zuordnung zwischen dynamischen IP-Adressen zu festen Domain-Namen erfolgt, wie für das

[606] Vgl. Summa: in Holznagel/Nelles/Sokol, TKÜV, S. 24.
[607] Siehe zu der Notwendigkeit von Telekommunikationsnetzen ebenso S. 25 ff.
[608] Vgl. zu diesem Begriff BfD-Info 5, Datenschutz in der Telekommunikation, 2001, S. 69. Siehe außerdem Schrey/Meister, K&R 2002, 177 ff.
[609] Zur Möglichkeit des Internetzugangs mittels Handy (Einwahl zum nächsten PoP) in einem VPN siehe Fn. 125.
[610] Vgl zu diesem Begriff oben S. 126.
[611] Vgl. zur Funktionsweise von DNS S. 30 ff.
[612] Köhntopp/Köhntopp, CR 2000, 248, 249.

herkömmliche DNS-Verfahren, mit Hilfe dessen feste IP-Adressen den entsprechenden Domain-Namen zugeordnet werden.[613]

Der DNS-Server übermittelt oder empfängt zwar nicht unmittelbar Nachrichten im Sinne von § 3 Nr. 22 TKG. Aber es handelt sich dennoch um eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG, da davon ebenso die Server zur Steuerung und Vermittlung von Online-Kommunikation erfasst sind.[614]
DNS ist letztendlich ein Verfahren,[615] was an der Erbringung der Access-Leistung mitwirkt,[616] wobei DNS-Server-Betreiber dementsprechend an der Erbringung eines Telekommunikationsdienstes gemäß § 3 Nr. 6 b) TKG mitwirken, da sie eine der Voraussetzungen für die Verständigung zwischen Sender und Empfänger schaffen. Zur Sicherstellung der Funktionstüchtigkeit des Internetzugangs muss notwendigerweise die Zuordnung zwischen IP-Adressen und Domain-Namen dauerhaft gespeichert werden.[617] Denn ohne DNS würde der Access nicht funktionieren und ohne Access wäre die DNS-Leistung überflüssig, so dass Access und DNS untrennbar miteinander verbunden sind.

Daher handelt es sich bei dem Betreiber eines DNS-Servers weder um einen Anbieter eines Teledienstes im Sinne von § 2 Abs. 2 Nr. 3 TDG[618] noch um einen „eigenständigen“ Telekommunikationsdienst, der mit der Tätigkeit eines Access-Providers gleichzusetzen wäre.[619]

---

[613] Zum dynamischen DNS-Server siehe S. 56.
[614] Unter den Begriff der Telekommunikationsanlagen nach § 3 Nr. 23 TKG fallen auch die Server und Router zur Steuerung und Vermittlung von Online-Kommunikation, siehe Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 2; Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 11; Wuermeling/Felixberger, CR 1997, 230, 233; Krader, Das neue Telekommunikationsrecht in der Praxis, S. 117: Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 87 TKG(1998), Band 1, Rn. 9. Siehe zum Begriff der Telekommunikationsanlage bereits S. 114
[615] Siehe Erwägungsgrund 28 der EU-Richtlinie 2002/58/EG.
[616] Vgl. auch § 3 Nr. 6 b) TKG, wonach "Diensteanbieter" jeder ist, der ganz oder teilweise geschäftsmäßig an der Erbringung solcher (Telekommunikations-)Dienste mitwirkt.
[617] Siehe S. 30 ff.
[618] OLG Hamburg, MMR 2000, 278, 278, siehe hierzu auch die Anmerkung von Spindler zu OLG Hamburg, MMR 2000, 278, 279. Siehe außerdem Tettenborn, MMR 1999, 516, 518; Koenig/Neumann, K&R 1999, 145, 149, die ebenfalls von einem Teledienst ausgehen.
[619] In diesem Sinne Spindler in seiner Anmerkung zu der Entscheidung des OLG Hamburg, MMR 2000, 278, 279. Siehe auch Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, S. 149 (in der 3. Auflage) und Tettenborn, MMR 1999, 516, 518, die die Vergabe der IP-Adressen, den DNS-Service sowie das Routing als Teledienst begreifen.

cc. Routing

Auch Routing[620] gehört zur notwendigen Internet-spezifischen Infrastruktur[621] und wird teilweise als Teledienst qualifiziert.[622]
Richtigerweise handelt es sich jedoch um einen Telekommunikationsdienst.[623] Router dienen lediglich dem Transport verschiedener Datenpakete im Internet[624] und stellen Telekommunikationsanlagen gemäß § 3 Nr. 23 TKG dar.[625] Routerbetreiber haben des Weiteren keine unmittelbare Kommunikationsbeziehung zu Nutzern im Internet, wie sie aber für die Anwendung des TDG/MDStV für erforderlich gehalten wird.[626]
Es fehlt insoweit an einem Angebot zur Nutzung des Internet oder anderer Netze, da kein Angebot an Nutzer erfolgt. Der Tatbestand des § 2 Abs. 2 Nr. 3 TDG ist damit nicht erfüllt.
Es kommt mangels eines bestimmten, angesprochenen Nutzers noch nicht einmal eine Zugangsvermittlung in Betracht,[627] da Leistungen der Routerbetreiber nur auf den Weitertransport von Daten zielen.[628]

In diesem Sinne wirken Routerbetreiber ebenso als Betreiber einer Telekommunikationsanlage an der Erbringung eines

---

[620] Siehe zur Funktionsweise von Routern S. 31.
[621] Köhntopp/Köhntopp, CR 2000, 248, 249.
[622] Tettenborn, MMR 1999, 516, 518; Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 83. Siehe auch Pankoke, Von der Presse- zur Providerhaftung, S. 56, der die Router-Rechner der Zugangsvermittlung zuordnet und diese als „Wegpunkte" für Datenpakete beschreibt, die entscheiden sollen, welche Route ein Datenpaket vom Absender zum Empfänger nimmt. Dies würde sich nach der obigen Definition eindeutig auf den Übertragungsvorgang beziehen, dennoch tendiert der Verfasser dazu, dies als Teledienst einzuordnen.
[623] Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 87/90; Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 46; Sieber in: Hoeren/Sieber, Teil 19 Rn. 242; Mecklenburg, ZUM 1997, 525, 526 ff.
[624] Koch, CR 1997, 193, 199.
[625] Siehe hierzu Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 2; Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 11. Siehe zum Begriff der Telekommunikationsanlage bereits S. 114 sowie S. 142.
[626] Beck-IuKDG-Tettenborn, § 2 TDG Rn. 40; Gola/Müthlein, TDDSG/TDG, § 2 TDG, S. 88. Zu eng ist jedoch die Auffassung des AG München, MMR 1998, 429 ff. („CompuServe"), die verlangt, dass eine Zugangsvermittlung Rechtsbeziehungen zu eigenen Kunden voraussetzen soll (AG München, MMR 1998, 429, 432); siehe hierzu auch die ablehnende Anmerkung von Sieber, MMR 1998, 438, 439.
[627] Vgl. Koch, Internet-Recht, S. 5, der anmerkt, dass Router-Rechner weder Zugang zum Web vermitteln noch Inhalte präsentieren. A.A. Pankoke, Von der Presse- zur Providerhaftung, S. 38, 44, der darauf verweist, dass Router unter den Anwendungsbereich des TDG fallen sollen, um eine Haftungsbefreiung zu erreichen.
[628] Vgl. auch Pankoke, Von der Presse- zur Providerhaftung, S. 41 mit dem Hinweis, dass den Routerbetreiber nur der so genannte Header der Datenpakete interessiert, also die Briefumschläge mit Absender- und Empfängeradresse.

Telekommunikationsdiensts gemäß
§ 3 Nr. 6 b) TKG mit.[629]

c. Relevanz des Telemediengesetzes?

Bei der oben vorgenommenen rechtlichen Betrachtung der Dienste als Teledienste oder Telekommunikationsdienstleistungen ist der Entwurf des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz- EIGVG) zu berücksichtigen. Unter dessen Artikel 1 ist das so genannte Telemediengesetz (TMG) geregelt.[630]
Das TMG führt den Begriff „ausschließlich“ ein.
So gilt nach § 1 Abs. 1 TMG dieses Gesetz für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht ausschließlich Telekommunikation nach § 3 Nr. 22 TKG darstellen.
Dies bedeutet, dass sich der Prüfungsansatz verschiebt, da nunmehr zu beurteilen ist, was unter „ausschließlich“ zu verstehen ist und ob Access-Providing demnach als Telemediendienst qualifiziert werden kann. Da die Gesetzesbegründung keinerlei Anhaltspunkte dafür liefert, wie „Ausschließlichkeit“ zu verstehen ist, müsste nun danach abgegrenzt werden, ob bei einer Access-Dienstleistung nur überwiegend oder ausschließlich die Telekommunikation bzw. der Übertragungsvorgang im Vordergrund steht. Denn zu berücksichtigen ist, dass auch Inhalte transportiert werden und insoweit ein Inhaltsbezug gegeben ist.
So wurde innerhalb der obigen Ausführungen[631] bereits darauf verwiesen, dass zwar der hauptsächliche Bezugspunkt in der Übertragung von Signalen besteht. Es war aber keine Prüfung erforderlich, inwieweit dieser Übertragungsleistung eine „absolute“ Ausschließlichkeit immanent ist oder ob Access-Providing lediglich überwiegend in der Übertragung von Signalen besteht und dies den Schwerpunkt der Leistung bildet.

---

[629] Gemäß § 3 Nr. 6 b) TKG gelten auch diejenigen als Diensteanbieter, die an der Erbringung von Telekommunikationsdiensten mitwirken.
[630] Der Gesetzentwurf ist abrufbar unter http://www.computerundrecht.de/docs/entwurf_eigvg_19_4_2005.pdf (Website vom 30.09.2006).
[631] Siehe S. 125 ff.

Die Beantwortung dieser Frage muss allerdings aus Raumgründen einer gesonderten Prüfung vorbehalten bleiben und kann in dieser Arbeit nicht abschließend beantwortet werden.
Folgendes soll jedoch allgemein zu dieser Thematik angemerkt werden: Sofern festgestellt werden sollte, dass im Sinne des TMG die Dienstleistung des Access-Providing nur überwiegend in der Übertragung von Signalen besteht, würde diese Dienstleistung grundsätzlich unter das Telemediengesetz fallen. Nichtsdestotrotz wäre aufgrund der Regelungen der §§ 14 Abs. 2, 15 Abs. 1 TMG dennoch in datenschutzrechtlicher Hinsicht das TKG anwendbar. Denn so regeln § 14 Abs. 2 und § 15 Abs. 1 TMG, dass das TKG bei Telemedien anwendbar bleibt, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Darüber hinaus wäre eine vertiefte Auseinandersetzung mit der Fragestellung erforderlich, ob die Regelungen des TMG einer Klarstellung dahingehend bedürfen, dass ebenso die Verarbeitung personenbezogener Dritter erlaubt ist, sofern deren schutzwürdige Interessen nicht entgegenstehen.[632]
Bedeutung hat dies ebenso für den Bereich der Datenschutzaufsichtsbehörde, da bei Anwendbarkeit des TMG auf Teledienste auch die Landesdatenschutzbehörden zuständig bleiben und nicht der Bundesbeauftragte für den Datenschutz. Nach § 8 TDDSG und § 38 BDSG unterstehen Anbieter von Telediensten den Aufsichtsbehörden, wohingegen für Telekommunikationsdienste der Bundesbeauftragte für Datenschutz zuständig ist.[633] Diese Folgerung resultiert daraus, dass anders als im Hinblick auf die datenschutzrechtlichen Vorgaben zum Umgang mit Daten (Bestands- und Nutzungsdaten) gemäß §§ 14, 15 TMG kein Verweis auf die geänderte Zuständigkeit erfolgt, so dass daraus geschlossen werden kann, dass die Zuständigkeit den Landesdatenschutzbehörden obliegen soll.
Der Vorteil einer solchen Auslegung bestünde in diesem Falle ebenso darin, dass die Aufsicht bei einer Stelle konzentriert ist und die funktionale und dienstorientierte Betrachtungsweise nicht zu einer Zersplitterung mit der Folge führt, dass unterschiedliche Dienstbestandteile eines kombinierten Dienstes von unterschiedlichen Behörden beaufsichtigt werden.

[632] In diesem Sinne Jandt, MMR 2006, 652 ff., insbesondere S. 656.
[633] Siehe hierzu S. 11.

Darüber hinaus ist gleichermaßen im Hinblick auf die in dieser Arbeit behandelten kombinierten Dienstleistungen zu prüfen, ob die funktionale und dienstorientierte Betrachtungsweise weiterhin Anwendung finden kann, oder ob der Gesetzgeber eine aus vielen Einzelleistungen kombinierte Dienstleistung in ihrer Gesamtheit bewerten möchte. Folge wäre, dass letztendlich doch ein Schwerpunkt der Dienstleistung gebildet werden müsste.
Dies hätte den Vorteil der Einzelfallbetrachtung im Sinne einer jeweils an der Praxis orientierten Auslegung. Der Nachteil bestünde aber darin, dass damit keine klare Abgrenzung zwischen Telekommunikationsdiensten und Telediensten möglich ist, sondern die Schwerpunktbildung einer Einzelfallbetrachtung obliegt.

2. Zwangsweises Tunneling

Um die datenschutzrechtlichen Anforderungen eines VPN vollumfänglich prüfen zu können, ist im Hinblick auf das so genannte zwangsweise Tunneling die Beurteilung notwendig, ob es sich hierbei um einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG oder einen Teledienst gemäß § 2 Abs. 1 TDG handelt. Beim zwangsweisen Tunneling muss der Provider auf dem Internetzugangsknoten, wie beispielsweise dem PoP, bzw. einem RADIUS-Server oder in einer Datenbank, auf die der Internetzugangsknoten[634] Zugriff nehmen kann, Identifikationsmerkmale eines VPN-Auftraggebers sowie dessen statische IP-Adresse speichern, um stets die Daten zu dem richtigen Standort übertragen zu können.[635]

Bei der Weiterleitung der Daten in das Unternehmensnetz des VPN-Auftraggebers steht der Transport und damit ein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG im Vordergrund. Insoweit ergeben sich hinsichtlich der Einordnung einer solchen Dienstleistung keine Unterschiede zum oben behandelten Access-Providing.

[634] Bei dem PoP handelt es sich um eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG, siehe Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 2; Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 11. Vgl. auch Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 85 TKG(1998), Band 1, Rn. 11.
[635] Siehe S. 57 ff.

Hiervon zu trennen ist die Frage, inwieweit für die Zuordnung und Festlegung der Identifikationsmerkmale auf dem Internetzugangsknoten bzw. in der entsprechenden Datenbank des Providers die Einwilligung des Kunden erforderlich ist bzw. nach welchen datenschutzrechtlichen Regelungen (§§ 91 ff. TKG oder BDSG) sich ein solcher Vorgang richtet. Dies soll jedoch an späterer Stelle unter den datenschutzrechtlichen Pflichten geprüft werden.[636]

3. VPN-Kommunikation

Die VPN-Kommunikation ist eine weitere Teilleistung des Gesamtpakets VPN, die einer Einordnung als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG oder Teledienst gemäß § 2 Abs. 1 TDG bedarf, um die notwendige Basis einer datenschutzrechtlichen Prüfung zu schaffen.
Diese Kommunikation ist von den Leistungen der Bereitstellung des Internetzugangs und der Leistung des zwangsweisen Tunneling abzugrenzen, da es hier um die Verbindung der einzelnen Standorte untereinander geht. Es werden weitere über die eigentliche Access-Dienstleistung hinausgehende Leistungen erbracht und weitere Technik eingesetzt. Daher muss geprüft werden, inwieweit diese weiteren Leistungen als Telekommunikationsdienst oder Teledienst einzustufen sind und welche Auswirkungen dies auf weitere datenschutzrechtliche Pflichten hat.
Im technischen Teil ist hierzu bereits dargestellt worden, dass es verschiedene Arten und Weisen gibt, ein VPN zu verwirklichen. Auf die dortigen Bildbeispiele und Beschreibungen wird daher verwiesen.[637]

In allen Fällen nehmen aber der Gateway beim Gateway-VPN oder der Server beim Software-VPN eine zentrale Rolle bei der Sicherstellung der VPN-Kommunikation ein.
So wird durch einen Gateway in einem Gateway-VPN die (Tele-) Kommunikation[638] sichergestellt. Der Gateway übernimmt insbesondere die Aufgabe, die Kommunikation in das jeweilige Unternehmensnetz

[636] Im Falle des zwangsweisen Tunneling muss der Access-Provider die Zuordnung zwischen Unternehmensstandorten kennen. Dies heißt, dass ihm bekannt sein muss, zu welchem Standort die Anfrage eines Unternehmensstandortes weitergeleitet werden soll. Siehe S. 226 ff.
[637] Siehe S. 44 ff.
[638] Telekommunikation ist nach § 3 Nr. 22 TKG der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen.

weiterzuleiten,[639] so dass es sich insgesamt um eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG handelt.[640] Entsprechendes gilt bei einem Software-VPN für den Rechner bzw. Server in der Firmenzentrale. Durch diesen wird die Telekommunikation im VPN zwischen den Nutzern sichergestellt,[641] so dass er insoweit eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG darstellt.[642]

Fraglich ist allerdings, ob und inwieweit der Provider bei den oben dargestellten Varianten der VPN-Kommunikation selbst einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG erbringt oder daran im Sinne von § 3 Nr. 6 b) TKG zumindest mitwirkt.[643] Ausgangspunkt dieser Fragestellung ist hierbei, ob der Provider beim Systemmanagement auch Betreiber dieses Systems (Gateway oder Rechner in der Firmenzentrale) ist, oder ob in diesem Falle nicht vielmehr der VPN-Auftraggeber als Betreiber des Gateways oder Servers gelten muss.

Die Klärung der Frage, wer bei einem Gateway-VPN Betreiber des Gateway oder bei einem Software-VPN Betreiber des Servers ist, ist von erheblicher Relevanz, da davon abhängt, inwieweit der Provider im Verhältnis zum Kunden Diensteanbieter eines eigenständigen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG ist und damit ebenso sowohl zum Datenschutz und zur Wahrung des Fernmeldegeheimnisses als auch gegebenenfalls zu Überwachungsmaßnahmen, die den Datenschutz gegenüber dem VPN-Auftraggeber beschränken, verpflichtet ist.[644]

---

[639] Siehe auch Sieber in: Hoeren/Sieber, Teil 1 Rn. 25/26: Der Host kann Daten nicht direkt an den Empfänger senden, sondern an einen Gateway oder Router, die dann die Weiterleitung übernehmen.

[640] Vgl. zur Funktion einer Telekommunikationsanlage auch Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 2; Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 11; Wuermeling/Felixberger, CR 1997, 230, 233; Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 85 TKG(1998), Band 1, Rn. 11. Siehe zum Begriff der Telekommunikationsanlage bereits S. 114, S. 142 sowie S. 143.

[641] Siehe das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch", S. 14, wo ausgeführt wird, dass ein Benutzer nach der erfolgreichen Anmeldung am directVPN mit anderen angemeldeten Computern Daten austauschen kann.

[642] Siehe zum weiten Begriffsverständnis des Begriffs der Telekommunikationsanlage S. 114 Fn. 492.

[643] Betreiber von Telekommunikationsanlagen wirken bei der Erbringung von Telekommunikationsdiensten mit und sind damit Diensteanbieter gemäß § 3 Nr. 6b) TKG (siehe hierzu Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 4).

[644] Siehe hierzu die Ausführungen in der Einführung S. 10 ff.

Der Betrieb des Gateway dient gerade der Erbringung eines Telekommunikationsdienstes bzw. dem Angebot von Telekommunikation und ist dessen technische Grundlage. Jeder Anbieter, der eine Telekommunikationsanlage im Sinne einer Funktionsherrschaft betreibt, ist damit auch Anbieter eines Telekommunikationsdienstes im Sinne von § 3 Nr. 6 TKG.

a. Funktionsherrschaft des VPN-Auftraggebers

aa. Komplettmanagement des Gateways durch den VPN-Auftraggeber

Aufbau und Funktionsweise eines solchen Komplettmanagements durch den VPN-Auftraggeber sind im technischen Teil dargestellt worden,[645] wobei im Folgenden die Frage eine Rolle spielt, inwiefern der VPN-Auftraggeber im rechtlichen Sinne der Betreiber der Telekommunikationsanlage „Gateway“ ist. Das Betreiben von Telekommunikationsanlagen wird zum einen lediglich als Ausübung der rechtlichen oder tatsächlichen Kontrolle (Funktionsherrschaft[646]) verstanden.[647] Zum anderen wird über diese Funktionsherrschaft hinaus verlangt, dass die Telekommunikationsanlagen dem Erbringen von Telekommunikationsdiensten dienen[648] müssen, wobei „dienen“ im Sinne eines tatsächlichen Nutzen im Rahmen des Erbringen von Telekommunikationsdiensten verstanden wird.[649]

Sofern der VPN-Auftraggeber das Gatewaymanagement in seinem Netzwerk bzw. Einflussbereich übernimmt, übt er auch die tatsächliche und rechtliche Kontrolle aus. Er hat die Funktionsherrschaft inne, da er die Möglichkeit hat, in eigener Verantwortung darüber zu entscheiden, ob die zu seinem lokalen

[645] Vgl. hierzu das Beispiel auf S. 50.
[646] Siehe auch § 3 Nr. 1 TKG a.F., der eine Legaldefinition zu der Funktionsherrschaft über Übertragungswege enthält.
[647] Geppert/Ruhle/Schuster, Handbuch der Telekommunikation, Rn. 778.
[648] Vgl. hierzu auch den Wortlaut von § 87 Abs. 1 TKG a.F. und § 109 Abs. 2 TKG, die den Betreiber von Telekommunikationsanlagen, welche dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen (§ 109 Abs. 2 TKG) bzw. welche dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen (§ 87 TKG a.F.), zu technischen Schutzmaßnahmen verpflichten. Siehe ebenso die Ausführungen auf S. 114.
[649] Ehmer in: TKG-Kommentar (2. Auflage), § 87 TKG Rn. 17, der im Zusammenhang mit dem Begriff „dienen“ darauf verweist, dass ein Bedürfnis für technische Schutzmaßnahmen nicht besteht, wenn eine Anlage tatsächlich nicht genutzt wird. Ebenso Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 31, der auf diese Ausführungen von Ehmer in der Vorauflage verweist.

Netzwerk führende Telekommunikationsanlage in Betrieb ist oder außer Betrieb gesetzt wird.[650]

Ausreichend ist hierbei, wenn sich die übertragungstechnischen Einrichtungen in rechtlicher und tatsächlicher Hinsicht unter der Kontrolle des Inhabers befinden.[651] Das Eigentum oder der Besitz ist hingegen nicht entscheidend.[652] Daher wäre unerheblich, wenn der VPN-Auftraggeber den Gateway vom Provider gemietet oder geleast hätte, sofern der Gateway im Machtbereich des VPN-Auftraggebers steht und dieser allein über dessen Betrieb oder Nichtbetrieb entscheiden kann. Sofern der Provider keine Zugriffsmöglichkeiten auf den Gateway hat, kann er auch keine Kontrolle über diesen ausüben. Selbst etwaige zwischen dem VPN-Auftraggeber und Provider vereinbarte Regelungen eines Miet- oder Leasingvertrages würden zu keiner anderen rechtlichen Beurteilung führen. Läuft der Vertrag beispielsweise aus oder behält sich der Provider ein Rückforderungsrecht bei ausbleibender Zahlung von Leasingraten vor, muss der VPN-Auftraggeber den Gateway zwar aus vertraglicher Sicht zurückgeben. Im Rahmen einer rechtlichen Betrachtung kann den vereinbarten vertraglichen Regelungen aber (wie stets) kein Vorrang vor den „wahren und gelebten“ Umständen eingeräumt werden.[653] Die wahren Umstände sind in diesem Falle, dass der Gateway dem Einflussbereich des Providers zunächst entzogen ist, wenn der VPN-Auftraggeber die Herausgabe verweigert. So kommt der VPN-Auftraggeber zwar seinen vertraglichen Rückgabepflichten nicht nach. Dies ändert aber nichts daran, dass der Provider in diesem Moment selbst keine Handhabe hat, den Gateway „abzuschalten“. Diese Entscheidung obliegt allein dem VPN-Auftraggeber, da der Gateway Teil seines Kommunikationsnetzes ist.

Hier entsteht also das Dilemma, dass eine vertraglich vereinbarte rechtliche Kontrolle nicht zu einer „wahren“ Funktionsherrschaft führt. Man kann in diesem

---

[650] Vgl. zu dem Begriff der Funktionsherrschaft im Zusammenhang mit dem Betrieb von Übertragungswegen Schütz in: TKG-Kommentar (2. Auflage), § 3 Nr. 1, Nr. 2 TKG Rn. 4/5; siehe außerdem Piepenbrock/Attendorn in: TKG-Kommentar (3. Auflage), § 16 TKG Rn. 23 ff. zum Betreiber eines Telekommunikationsnetzes.

[651] Bothe/Heun/Lohmann, ArchivPT 1995, 5, 18/20, die für den Fall des Betreibers eines Übertragungsweges ausführen, dass es für die Stellung des Betreibers grundsätzlich auf die rechtliche und tatsächliche Herrschaft gegenüber den Nutzern ankomme, wobei Eigentumsverhältnisse nicht entscheidend sind.

[652] Schütz in: TKG-Kommentar (2. Auflage), § 6 TKG Rn. 34; in diesem Sinne auch Piepenbrock/Attendorn in: TKG-Kommentar (3. Auflage), § 16 TKG Rn. 23.

[653] Vgl. zum Widerspruch zwischen der praktischen Tätigkeit und der schriftlichen Vereinbarung im Arbeitsverhältnis Wedde, Telearbeit, S. 39 unter Verweis auf die Entscheidung des BAG v. 24.06.1992 AP Nr. 61 zu § 611 BGB Abhängigkeit.

Zusammenhang ebenso wenig von „Herrschaft“ reden, wenn der VPN-Auftraggeber erst durch eine gerichtliche Entscheidung zur Herausgabe gezwungen werden müsste. Die „Herrschaft“ des Providers ist zwischenzeitlich verlorengegangen, ansonsten hätte er sofort die Möglichkeit gehabt, den Gateway außer Betrieb zu nehmen. Daher muss sich das Merkmal der „Herrschaft“ vielmehr an den tatsächlichen Einflussmöglichkeiten und Umständen und nicht an einem Vertragstext orientieren.

In diesem Sinne ist der VPN-Auftraggeber und nicht der Provider Betreiber des Gateways. Der Gateway kann ihm daher für das Erbringen eines Telekommunikationsdienstes gemäß § 3 Nr. 24 TKG „dienen“, was im Folgenden, und zwar im Verhältnis zum Nutzer des VPN, noch zu untersuchen sein wird.[654] Welche Konsequenzen dies insgesamt für den Datenschutz, insbesondere für die Frage der Auftragsdatenverarbeitung hat, wird gemäß der Aufbaulogik dieser Arbeit an späterer Stelle untersucht.[655]

Einerseits müssen in diesem Kontext Datenvermeidung, Sicherstellung der technischen Schutzmaßnahmen sowie etwaige Auskunfts- und Überwachungsmaßnahmen „bei“ der Diensterbringung beurteilt werden. Hier steht der Datenschutz des jeweiligen Nutzers im Fokus der Betrachtung.[656] Andererseits ist aber gleichermaßen die Frage der Datenverarbeitung auf dem Gateway entscheidend, so dass die datenschutzrechtlichen Interessen eines weiteren Beteiligten der VPN-Kommunikation betroffen sind (Betroffener).[657] Für eine datenschutzrechtliche Gesamtaussage muss daher eine Prüfung in dem jeweiligen einschlägigen Personenverhältnis vorgenommen und zwischen den Interessen des Nutzers und des Betroffenen unterschieden werden. Dabei muss insbesondere berücksichtigt werden, ob der VPN-Auftraggeber oder der Provider zur Umsetzung von datenschutzrechtlichen Anforderungen verpflichtet ist.[658]

[654] Dies wird auf S. 302 ff. näher ausgeführt.
[655] Siehe hierzu die Verweise unter Fn. 658.
[656] Siehe zum Begriff des Nutzers S. 83 ff.
[657] Siehe zum Begriff des Betroffenen S. 85 ff.
[658] Siehe S. 231 ff., 290 ff., 352 ff., 403 ff., 449 ff. Siehe insbesondere auch S. 453 (Personenverhältnis “Provider/Betroffener”), wo nochmals deutlich auf die Unterschiede zwischen Funktionsherrschaft und Auftragsdatenverarbeitung hingewiesen wird.

bb. Splitmanagement im Machtbereich des VPN-Auftraggebers

Aufbau und Funktionsweise des so genannten Splitmanagement im Sinne eines Servicemanagement des Gateways (d.h. regelmäßige Wartung, Fernwartung[659] oder Serviceleistungen, wie etwa das Aufspielen von Updates) sind im technischen Teil dargestellt worden.[660]
Auch in diesem Falle verbleibt die Funktionsherrschaft über den Gateway beim VPN-Auftraggeber, sofern der Provider das Splitmanagement, übernimmt. Dies folgt wiederum aus der im vorherigen Prüfungspunkt „Komplettmanagement" dargestellten Argumentation,[661] dass der Gateway im Machtbereich bzw. räumlichen Einflussbereich des VPN-Auftraggebers steht. Ist der Gateway (wie bei dieser Variante) in das Gesamtnetzwerk des VPN-Auftraggebers integriert, kann dieser folglich darüber entscheiden, ob und zu welchem Zeitpunkt der Gateway außer Betrieb genommen wird, beispielsweise weil Wartungsarbeiten oder die Sicherheit seines Gesamtnetzwerkes dies erfordert. Der VPN-Auftraggeber hat damit die alleinige Einflussmöglichkeit und die Funktionsherrschaft inne.

Zwar kann einem zu Recht der Gedanke kommen, ob ein Provider aufgrund seines tatsächlichen technischen Wissensvorsprungs nicht stets die tatsächliche Kontrolle über Betrieb und Nichtbetrieb der Anlage innehat, sofern der VPN-Auftraggeber das Systemmanagement (teilweise) aus der Hand gibt und sich auf den (Wartungs-)Service des Providers vollumfänglich verlässt und diesem vertraut. Aber dieser technische Wissensvorsprung führt nicht dazu, dass der VPN-Auftraggeber die tatsächliche Kontrolle über den Betrieb oder den Nichtbetrieb der Telekommunikationsanlage verliert, wenn diese in seinen Räumlichkeiten untergebracht ist und in sein Netzwerk integriert ist.[662] Wenn er im Einzelfall einem Ratschlag des Providers Folge leistet und den Gateway abschaltet, weil dies aus technischen Gründen sinnvoll ist, bedeutet dies im Umkehrschluss nicht, dass er die tatsächliche Verfügungsmacht vollumfänglich verliert. Der VPN-Auftraggeber kann nach wie vor selbständig über den Betrieb oder Nichtbetrieb des Gateway entscheiden. Etwas anderes gilt nur im Falle

[659] Siehe zum so genannten „Remote Access" auch Bischof/Witzel, ITRB 2003, 31, 37.
[660] Siehe S. 51 ff.
[661] Siehe oben S. 150 ff.
[662] Vgl. Bothe/Heun/Lohmann, ArchivPT 1995, 5, 18/20.

eines bewussten Sabotageakts durch den Provider, der zum Ausfall des Systems führt. Damit wird jedoch der Provider nicht zum „Funktionsherr“ im Sinne des Gesetzes. Ein solcher Sabotageakt ist vielmehr mit sämtlichen Systemangriffen von außen gleichzusetzen. Ein Saboteur erhält zwar eine gewisse Machtfunktion. Er wird dadurch aber nicht zum Betreiber einer Telekommunikationsanlage, da er selbst keine Telekommunikationsdienste erbringt. Zudem wird ein Saboteur regelmäßig im Falle einer Sabotage auch keine weitere Möglichkeit haben, den Gateway wieder in Betrieb zu nehmen, da im weitere Zugriffe verwehrt werden würden (was damit ebenso gegen eine Funktionsherrschaft spricht).
Der Provider ist in diesem Falle damit kein Telekommunikationsdiensteanbieter nach § 3 Nr. 6 b) TKG, da die Telekommunikationsanlage nicht dem Erbringen eines Telekommunikationsdienstes gemäß § 3 Nr. 24 TKG durch ihn dient.
Ist der Gateway allein für den VPN-Auftraggeber eingerichtet und steht in dessen räumlichen Einflussbereich, wodurch die Kontrollmöglichkeit des Providers in tatsächlicher Hinsicht zwangsläufig eingeschränkt ist, so muss von einem Betrieb der Telekommunikationsanlage durch den VPN-Auftraggeber ausgegangen werden. Dies gilt auch, sofern er die Anlage von dem Provider lediglich gemietet hat.

cc. Software-VPN

Beim Software-VPN übt der VPN-Auftraggeber regelmäßig die Funktionsherrschaft über den Rechner bzw. Server aus, auf welchem die VPN-Software, inklusive Benutzerverwaltung, installiert ist.[663] Dieser Rechner stellt insoweit eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG dar,[664] da er die Basis für die Kommunikation zwischen den VPN-Nutzern darstellt.
Auch hier muss dem VPN-Auftraggeber die Entscheidung darüber vorbehalten bleiben, ob sein Gesamtnetzwerk gegebenenfalls außer Betrieb zu nehmen ist. Der Provider ist damit bei einem Software-VPN kein Anbieter eines Telekommunikationsdienstes gemäß § 3 Nr. 24 TKG, auch wenn er beispielsweise im Wege der Fernwartung regelmäßige Updates oder sonstige Servicepacks liefern würde.

[663] Siehe zum Aufbau und Funktionsweise des Software-VPN S. 53.
[664] Siehe oben S. 148.

b. Funktionsherrschaft des Providers

aa. Komplettmanagement durch den Provider

Etwas anderes ergibt sich aber dann, sofern sich der Gateway im kompletten Machtbereich des Providers befindet (Aufbau und Funktionsweise des Komplettmanagement durch den Provider sind im technischen Teil dargestellt worden.)[665]
So besteht die Möglichkeit, den Gateway nebst Sicherheitsfunktionen vom Provider betreiben zu lassen, so dass dieser etwa auf Nutzernamen, Passwörter zugreifen kann bzw. die Benutzerverwaltung vornimmt.[666] Der Provider ist hierbei für die Sicherheit des Gateways verantwortlich.[667]

In diesem Fall hat sich die Dienstleistung rechtlich verselbständigt.[668] Der Gateway steht im räumlichen Einflussbereich des Providers und ist regelmäßig in dessen Netz bzw. Netzwerk integriert.[669]
Der Kunde kann tatsächlich keinen Einfluss auf den Gateway ausüben und hat keine Verfügungsmacht.
Der Provider möchte und muss hier regelmäßig selbst über dessen Betrieb oder Nichtbetrieb entscheiden, um die Funktionstauglichkeit seines (Gesamt-) Systems sicherstellen zu können. Er hat damit die Funktionsherrschaft inne.
Für die Frage der Funktionsherrschaft kann auch hier nicht die Frage der Vertragsausgestaltung und etwaiger zwischen Provider und VPN-Auftraggeber vertraglich vereinbarter Regelungen interessieren.[670] Zwar wird im Rahmen der Definition der Funktionsherrschaft auf die tatsächliche **und** rechtliche Kontrolle verwiesen und diesen Merkmalen damit gleiche Relevanz zugemessen.[671] Es

[665] Siehe S. 49 sowie das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 239 ff. Zur Ausgliederung von IT-Leistungen siehe Voßbein, RDV 1993, 205 ff., der die Auslagerung der Datenverarbeitung unter betriebswirtschaftlichen Gesichtspunkten betrachtet und auf den Begriff des „Lean Management“ hinweist. Siehe auch Müthlein, RDV 1993, 165, 170, der in diesem Zusammenhang auf „externes Outsourcing“ verweist.
[666] Siehe oben S. 49. Insbesondere kommt hier auch in Betracht, dass ein (einziges) Gateway (im hardwaretechnischen Sinne) mehreren Kunden zur Verfügung steht, wobei jedoch die Datenverarbeitung stets getrennt für den jeweiligen Kunden abläuft.
[667] Siehe das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 239 ff.
[668] Der Provider hat in rechtlicher und tatsächlicher Hinsicht die Kontrolle über den Gateway, siehe auch Bothe/Heun/Lohmann, ArchivPT 1995, 5, 18/20.
[669] Siehe das Bildbeispiel im Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 239.
[670] Siehe oben S. 150 ff.
[671] Siehe zur Definition S. 149.

sind jedoch die „wahren und gelebten" Umständen im Rahmen einer rechtlichen Betrachtung zu berücksichtigen. Die wahren Umstände sind in diesem Falle, dass der Gateway dem Einflussbereich des VPN-Auftraggebers vollständig entzogen ist. Dies gilt, selbst wenn vertraglich vereinbart ist, dass der Provider eine 99,99 prozentige Verfügbarkeit garantiert und für den Ausfall des Gateway haftet. Schaltet der Provider eigenmächtig den Gateway ab, beispielsweise weil er dringende und dem Vertrag in zeitlicher Hinsicht widersprechende Wartungsarbeiten durchführt, so macht er sich zwar unter Umständen schadensersatzpflichtig und kommt seinen Gewährleistungspflichten nicht nach. Dies ändert aber nichts daran, dass der VPN-Auftraggeber in diesem Moment selbst keine Handhabe hat, den Gateway wieder in Betrieb zu nehmen. Diese Entscheidung obliegt dem Provider und eine vertraglich zugesicherte rechtliche Kontrolle führt auch hier nicht zu einer „wahren" Funktionsherrschaft. Selbst wenn der Provider durch eine gerichtliche einstweilige Verfügung zur (Wieder)Inbetriebnahme gezwungen werden würde, wäre die „Herrschaft" zwischenzeitlich verlorengegangen. Daher muss bei der Betrachtung der Schwerpunkt ebenso auf die tatsächliche Kontrolle und nicht die rechtliche Kontroll**möglichkeit** gelegt werden.[672]

Der Provider betreibt infolgedessen selbständig eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG, die den Anforderungen des § 88 TKG und § 109 Abs. 1 TKG entsprechen muss, und die ebenso einem vom ihm erbrachten Telekommunikationsdienst gemäß § 3 Nr. 24 TKG dient. Der Provider ist ebenso Diensteanbieter gemäß § 3 Nr. 6 b) TKG und ist damit zur Wahrung des Fernmeldegeheimnisses gemäß § 88 TKG verpflichtet, was aber an späterer Stelle unter den datenschutzrechtlichen Pflichten näher zu untersuchen ist.[673]

[672] Siehe insbesondere auch S. 453 (Personenverhältnis "Provider/Betroffener"), wo nochmals deutlich auf die Unterschiede zwischen Funktionsherrschaft und Auftragsdatenverarbeitung hingewiesen wird.
[673] Vgl. hierzu S. 250 ff.

bb. Splitmanagement im Machtbereich des Providers

Oben wurde die Variante des Splitmanagement dargestellt, bei welcher der Gateway im räumlichen Einflussbereich des VPN-Auftraggebers integriert ist, und der Provider „lediglich“ Wartungs- bzw. Fernwartungsleistungen erbringt.[674] Es gibt beim Splitmanagement außerdem die folgende weitere mögliche Variante: Der Gateway befindet sich im räumlichen Einflussbereich des Providers und ist in dessen Netzstruktur integriert .Der VPN-Auftraggeber kann dennoch durch Fernzugriff Administrationsrechte ausüben.[675]

Auch für diese Fallgestaltung muss entsprechend der obigen Ausführungen gelten, dass der Provider Betreiber des Gateway ist, sofern sich dieses in dessen räumlichen Einflussbereich bzw. Machtbereich befindet und in dessen Netzwerk integriert ist.[676]
Dies ist insbesondere mit der Servermiete[677] vergleichbar. Denn sofern eine Anlage in einem fremden Rechenzentrum integriert ist und einem Kunden nur als Speicherplatz überlassen wird, sorgt dieses Rechenzentrum zwar „nur“ aber auch mindestens für die Einsatzbereitschaft des Systems. Daher werden in diesem Falle vertragliche Regelungen die tatsächlichen Umstände wiedergeben und bestätigen. So muss sich der Provider vorbehalten, die Anlage abzuschalten, sofern die Betriebssicherheit oder Wartungsarbeiten dies erfordert, weil und sofern dies zur Erhaltung und zum Schutz der Anlage notwendig ist oder Einfluss auf sein gesamtes Netzwerk hat. So gehört es zu den Pflichten eines Anbieters, einen Server des Kunden, der bei ihm untergestellt ist an seine Netzwerkanbindung ins Internet anzuschließen, regelmäßig dessen Wartung und Pflege zu übernehmen und den Anschluss auf dessen einwandfreies Funktionieren hin zu überprüfen.[678] Der Anbieter haftet für technische Defekte, sofern er die technische Versorgung nicht bestmöglich erfüllt, für Ausfälle durch Virenbefall und Hackerangriffe, wobei erhöhte Sicherungs- und Schutzmaßnahmen nur gegen gesonderte Vergütung vom

[674] Siehe S. 152.
[675] Siehe S. 52.
[676] Siehe oben S. 150 ff./S. 154.
[677] Vgl. hierzu v.Sponeck, CR 1992, 594, 594.
[678] Vgl. hierzu außerdem Wulf, CR 2004, 43, 46, der dies im Falle des so genannten Serverhousing in Bezug auf Serververträge und der Haftung eines Anbieters für Ausfälle feststellt.

Anbieter zu erfüllen sind.[679] Aus diesen zivilrechtlichen Überlegungen ergibt sich ebenso, dass letztendlich der Anbieter die Kontrolle über einen Server hat, soweit er in seinen Räumlichkeiten bzw. Machtbereich steht. In den Vertragsbestimmungen zwischen VPN-Auftraggeber und Provider sollten daher ebenso Regelungen enthalten sein, die zum Schutze des VPN-Auftraggebers zumindest gewisse Verfügbarkeitslevels des Gateway zusichern.

Damit ergibt sich insgesamt, dass derjenige die Kontrollmöglichkeit behält, in dessen Netzwerkumgebung sich der Gateway befindet. Der Provider erbringt durch den Betrieb des Gateways und durch die Weiterleitung der Daten vom Gateway ins Firmennetz des VPN-Auftraggebers einen eigenständigen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG und ist Diensteanbieter gemäß § 3 Nr. 6 b) TKG.

4. Zusatzdienst E-Mail

Der E-Mail-Dienst gehört im eigentlichen Sinne nicht zu einem VPN im engeren Sinne, stellt vielmehr einen Zusatzdienst dar, da das VPN gerade den E-Mail-Verkehr zwischen den Unternehmensstandorten ersetzen soll.[680]
Dennoch wird ein Provider, der ein Internet-VPN bereit stellt und damit für den Internetzugang Sorge trägt, regelmäßig auch die Einrichtung von E-Mail-Accounts sowie entsprechenden Mailservern, die für die Weiterleitung der E-Mails verantwortlich sind, übernehmen.[681] Daher ist zu unterscheiden, inwieweit TDDSG oder TKG zu berücksichtigen und E-Mail-Daten zu löschen sind.
Zu betonen ist, dass die nachfolgenden Ausführungen entsprechend der Darstellungen zu den Dienstleistungen einer Internetverbindung (Internet-Access, TK-Providing, Routing und DNS-Service)[682] für sämtliche Nutzer und Teilnehmer eines E-Mail-Dienstes und nicht VPN-spezifisch gelten. Etwas anderes gilt nur, soweit im Verlauf der Prüfung eine Besonderheit in einem VPN

[679] Wulf, CR 2004, 43, 47/48.
[680] Siehe zum E-Mail-Dienst in Verbindung mit einem VPN S. 3, insbesondere Fn.16 in dieser Arbeit.
[681] Siehe hierzu S. 3 und Schneider, Verträge über Internet-Access, S. 97 ff.; Cichon, Internetverträge, Rn. 121 ff.
[682] Siehe S. 120 ff., 162 ff.

hervorgehoben wird. Dies betrifft gleichermaßen die anschließende datenschutzrechtliche Prüfung.[683]

Im Sinne der dienstorientierten Betrachtungsweise ist dieser Zusatzdienst zunächst von den anderen Dienstleistungen des VPN gesondert zu betrachten.[684] Gemäß der funktionalen Betrachtungsweise ist bei dieser Einzelleistung eines kombinierten Online-Dienstes darüber hinaus die Einordnung des E-Mail-Service als Telekommunikationsdienst oder Teledienst erforderlich, wobei im Sinne der obigen Ausführungen funktional zwischen Transport- und Inhaltsebene zu trennen ist.[685]

Aus dieser Betrachtungsweise ergibt sich, dass die Übertragung der E-Mail bzw. der „Übertragungsvorgang an sich" als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG einzuordnen ist,[686] was im Folgenden näher begründet wird. Gemäß der obigen Ausführungen stellt die gesetzliche Begriffsdefinition des § 3 Nr. 24 TKG hierfür nicht nur die entscheidende, sondern auch eine ausreichende Grundlage dar.[687] Denn im Verhältnis zwischen Provider und VPN-Auftraggeber stehen nicht die Inhalte an sich im Vordergrund, sondern vielmehr die Übertragung der Inhalte. Dies gilt sowohl für den Vorgang des Versendens als auch für den Abruf der Inhalte vom Mailserver des Providers.[688]

[683] Siehe die datenschutzrechtliche Prüfung auf S. 269 ff.
[684] Siehe zur dienstorientierten Betrachtungsweise S. 74/86.
[685] Siehe zur funktionalen Betrachtungsweise insbesondere die Ausführungen auf S. 66 ff. sowie den Hinweis auf S. 74, dass die Trennung in eine Transport- oder Inhaltsebene im Rahmen einer Einzelleistung weiterhin erforderlich ist.
[686] Kieper, DuD 1998, 583, 584 ff.; Schmitz in Hoeren/Sieber, Teil 16.4 Rn. 44/45; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 89/90; Krader in: Königshofen, Das neue Telekommunikationsrecht in der Praxis, S. 121/122.
[687] Siehe hierzu S. 126.
[688] Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 92 führt richtigerweise aus, dass Ausgangspunkt jeder Kommunikationsmöglichkeit über E-Mail der Anschluss an Datenleitungen ist. Gegenstand des Vertrages zwischen Provider und Kunden ist auf der einen Seite die Berechtigung des Kunden, den Netzanschluss zu nutzen, auf der anderen Seite die Verpflichtung des Providers den Anschluss zu bestimmten technischen Bedingungen bereit zu halten (Kleine-Voßbeck aaO). Hier vermengt der Verfasser zwar die Bereitstellung des Internetzugangs mit der Bereitstellung des Dienstes, der sich auf die Übertragung von E-Mails bezieht, wobei die jeweiligen Provider im Übrigen nicht identisch sein müssen (vgl. das Bildbeispiel auf S. 63 in dieser Arbeit). Richtig ist jedoch, dass auch der Anbieter, der E-Mails über das Internet transportiert ohne den Access-Provider keine Chance hat, seinen Dienst bereit zu stellen. Siehe hierzu auch die technischen Ausführungen auf S. 62 ff. sowie die Ausführungen von Schaar, Datenschutz im Internet, Rn. 266 ff., der darauf hinweist, dass nunmehr auch das Bundeswirtschaftsministerium sowie die Bundesnetzagentur, zu dem Schluss gekommen seien, dass es sich bei der E-Mail-Kommunikation um einen Telekommunikationsdienst handelt, und zwar mit der Konsequenz, dass die

Zwischen VPN-Auftraggeber und Provider findet keine Individualkommunikation im Sinne von § 2 Abs. 2 Nr. 1 TDG statt. Aus Sicht des VPN-Auftraggebers ist vielmehr ausschlaggebend, dass die Übertragung der E-Mails funktioniert.[689] Der Provider stellt dem VPN-Auftraggeber lediglich eine technische Möglichkeit zur Verfügung, die dieser in Anspruch nehmen kann, um Daten zu empfangen oder weiterzuleiten, womit es sich um Telekommunikation gemäß § 3 Nr. 23 TKG handelt.

Dies wird insbesondere an der obigen Abbildung[690] deutlich. Diese zeigt, dass ein Mailserver vorhanden ist, auf welchem die E-Mails für den Empfänger zum Abruf gespeichert werden (POP3-Mailserver), wobei ein weiterer Mailserver (SMTP-Mailserver) beim Versand für die Weiterleitung und kurzzeitige Zwischenspeicherung der E-Mails verantwortlich ist.

Beide Mailserver können von demselben Provider betrieben werden, je nachdem ob Sender und Empfänger der E-Mail mit demselben Provider ein Vertragsverhältnis eingegangen sind. Entscheidend ist aber, dass sowohl beim Versenden einer E-Mail als auch beim Abruf einer E-Mail die transportbezogene Weiterleitungsfunktion im Vordergrund steht.

Der Provider stellt zwar durch die Speicherung der E-Mails auf seinem POP3-Server Daten zum Abruf bereit, bei diesen Daten handelt es sich jedoch nicht um eigene Inhalte bzw. Informationen des Providers, so dass das eigentliche Angebot des Providers an den VPN-Auftraggeber darin besteht, ihm fremde Daten zu übermitteln.[691] Die Bereitstellung einer Telekommunikationsmöglichkeit im Sinne von § 3 Nr. 23 TKG liegt gleichermaßen bei Verwendung des Protokolls IMAP vor.[692] Denn hier eröffnet der Provider dem Nutzer ebenso (nur) ein Mittel zur Kommunikation und zum Datentransport, hier allerdings unter der zusätzlichen

Kommunikationsinhalte direkt an das einfachgesetzliche, strafbewehrte Fernmeldegeheimnis gebunden sind.

[689] Bei dem E-Mail-Dienst ergibt sich zudem die Besonderheit, dass er gleichzeitig aufgrund seiner spezifischen Protokolle einen Internet-Dienst darstellt (siehe auch S. 76). Aber aufgrund des Angebots eines Providers, den E-Mail-Service einzurichten und die Voraussetzungen für den Zugang zu schaffen, ist dieser Dienst darüber hinaus ein Dienst im Sinne der Informationsgesellschaft (vgl. hierzu etwa Beck-IuKDG-Tettenborn, § 2 TDG Rn. 39) und ein Telekommunikationsdienst.

[690] Siehe S. 63.

[691] Siehe hierzu auch die obigen Argumente im Hinblick auf das Access-Providing, S. 129 ff. unter Hinweis darauf, dass es stets notwendig ist, dass der Anbieter eines Teledienstes Inhalte bereithält.

[692] Siehe zu IMAP S. 62.

Möglichkeit des umgekehrten Weges, indem der Nutzer selbständig Daten auf den Server übertragen kann bzw. Daten auf dem Server ändern kann.

Daraus folgt also, dass es sich beim E-Mail-Dienst im Verhältnis zwischen Provider und VPN-Auftraggeber um einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG handelt. Wenn hingegen die Ansicht vertreten wird, dass das Versenden und Empfangen einer E-Mail einen Teledienst darstellt,[693] muss im Sinne der gesetzlichen Intention auf das richtige Personenverhältnis abgestellt werden.[694] Lediglich im Hinblick auf denjenigen, mit denen der VPN-Auftraggeber E-Mails austauscht, können die übermittelten Inhalte entscheidend sein und nicht der funktionierende technische Übertragungsvorgang im Vordergrund stehen. Nur in diesem Fall kann es sich daher gegebenenfalls um Individualkommunikation nach § 2 Abs. 2 Nr. 1 TDG handeln, was in dem Personenverhältnis „VPN-Auftraggeber und Nutzer“ untersucht werden soll.[695] Daher zeigt sich auch an dieser Stelle wieder, dass die Betrachtung des Mehrpersonenverhältnisses für eine vollumfängliche datenschutzrechtliche Betrachtung wichtig ist.
Aber selbst wenn in dem Personenverhältnis „VPN-Auftraggeber/Nutzer“ ein Teledienst gemäß § 2 Abs. 2 Nr. 1 TDG bejaht werden sollte, wird der Provider nicht zum Teledienstanbieter gemäß § 3 Nr. 1 TDG (Bereithalten von fremden Inhalten auf seinem Server).
Dies folgt daraus, dass gemäß § 2 Abs. 4 Nr. 1 TDG das Teledienstegesetz nicht für Telekommunikationsdienste gilt, wobei entscheidend ist, dass der Provider zwangsläufig Absender- und Zieladresse sowie Kommunikationsinhalt auf seinem Server zwischen speichern muss.[696] Die Speicherung der E-Mail-Kommunikation auf den Mailservern des Providers ist für die E-Mail-Übertragung unbedingt notwendig und deren zwangsläufige technische Voraussetzung ist.[697] So hat die Speicherung nur solange Bedeutung, wie sie

[693] Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 89.
[694] Vgl. auch Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I Rn. 60, der den E-Mail-Dienst als reinen Teledienst betrachtet, aber dabei nicht auf das jeweilige Personenverhältnis eingeht.
[695] Siehe hierzu S. 315 ff. sowie die Definition des Nutzers auf S. 83.
[696] Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 122 unter dem Hinweis, dass die Speicherung der Netz-Benutzungsdaten eine zwangsläufige technische Voraussetzung für die Abwicklung der Versendung elektronischer Post ist.
[697] Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 122. Siehe auch Glatt, Vertragsschluss im Internet, S. 23 und dem Hinweis, dass der Unterschied zwischen E-Mail und WWW allein darin bestehe, dass beim E-Mail-Verkehr im Regelfall keine unmittelbare

für die Ausführung des Dienstes erforderlich ist.[698] Eine Speicherung über diesen Zeitpunkt würde darüber hinaus die Gefährdung einer Kenntnisnahme durch unbefugte Dritte erhöhen.[699]

Damit steht allerdings eindeutig die Funktionsfähigkeit des Übertragungsvorgangsvorgangs, und zwar anwendungsdiensteunabhängig,[700] im Vordergrund. Daher muss es ebenso in diesem Falle bei der rechtlichen Einordnung des E-Mail-Dienstes als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG in dem hier untersuchten Personenverhältnis „Provider/VPN-Auftraggeber“ bleiben.

Übertragung der Daten vom PC des Absenders auf den Rechner des Empfängers, sondern eine Zwischenspeicherung auf den Servern des Providers erfolgt. Aus diesen Ausführungen wird auch ersichtlich, dass der Datenabruf vom Mailserver des Providers lediglich eine notwendige technische Voraussetzung ist. Vgl. hierzu auch Sieber in: Hoeren/Sieber, Teil 19 Rn. 143 Fn. 1 mit der Darstellung, dass im Bereich der E-Mail zunächst zwischen der Speicherung ankommender Nachrichten der oft nur kurzfristigen Speicherung abgehender Nachrichten zu unterscheiden ist. Sieber (aaO) verweist außerdem darauf, dass eingehende E-Mails nicht zwingend bis zum Abruf durch den Empfänger auf dem Mailserver gespeichert, sondern in ein zentrales Verzeichnis gestellt werden. Die Verweildauer in solchen Verzeichnissen hängt dabei vom jeweiligen Provider ab, ist aber umso kürzer je größer die Zahl der Mails sei, die versendet werden sollen (vgl. Sieber aaO).

[698] Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 122.

[699] Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 122, der hier auch auf das Recht auf informationelle Selbstbestimmung verweist.

[700] Vgl. hierzu auch S. 126.

II. Datenschutz innerhalb der Dienste im VPN

Bei der Beurteilung der datenschutzrechtlichen Erfordernisse interessieren die im zweiten Abschnitt dargestellten datenschutzrechtlichen Pflichten .[701]
Zunächst ist also zu prüfen, welche Daten auf den einzelnen an der Bereitstellung eines VPN beteiligten Systemen anfallen können und ob und wie dieser „Datenanfall" vermieden werden kann.
Des Weiteren ist in dem hier zugrunde gelegten Personenverhältnis VPN-Auftraggeber und Provider ebenso zu prüfen, welcher dieser beiden Beteiligten für die Systemsicherheit und damit für die technischen Schutzmaßnahmen auf dem jeweiligen System (Gateway) verantwortlich ist.
Darüber hinaus ist im Sinne einer vollumfänglichen datenschutzrechtlichen Prüfung zu untersuchen, inwiefern der Datenschutz und die Datensicherheit durch die Erfüllung von gesetzlichen Überwachungspflichten beschränkt sein könnten.

Die Prüfungsreihenfolge orientiert sich wiederum an der hier entwickelten (und gleichermaßen aus dem Inhaltsverzeichnis ersichtlichen) dienstorientierten Betrachtungsweise.[702] In Übereinstimmung mit der oben vorgenommenen rechtlichen Einordnung der einzelnen Dienstleistungen[703] des (kombinierten Online-Dienstes) VPN Telekommunikationsdienste erfolgt im Folgenden die datenschutzrechtliche Betrachtung dieser (Einzel-)Dienstleistungen.

1. Internetverbindung

Es wird (entsprechend der Prüfung unter I.)[704] als erster Punkt die aus den Dienstleistungen des Access-Providing, TK-Providing, DNS-Service sowie Routing bestehende Dienstleistung „(Herstellen einer) Internetverbindung" geprüft. In diesem Rahmen werden (entsprechend der Aufbaulogik dieser Arbeit) die Fragen der Datenvermeidung, gesetzlichen Unterrichtungspflichten,

[701] Siehe S. 106 ff.
[702] Siehe zur dienstorientierten Betrachtungsweise S. 74/86.
[703] Siehe zu den einzelnen relevanten Dienstleistungen des VPN S. 120 ff.
[704] Vgl. S. 121 ff.

Technischen Schutzmaßnahmen sowie die Schranken des Datenschutz behandelt. [705]

Die Besonderheit liegt bei den nachfolgenden Ausführungen darin, dass diese für sämtliche Nutzer und Teilnehmer einer Internetverbindung und nicht VPN-spezifisch gelten. Etwas anderes ergibt sich nur, soweit im Verlauf der Prüfung eine Besonderheit in einem VPN hervorgehoben wird.

a. Access-Providing

aa. Datenvermeidung

Im Folgenden wird die Verpflichtung zur Datenvermeidung hinsichtlich IP-Adressen als Tunnel-Startpunkte und Tunnel-Endpunkte untersucht.

Eine IP-Adresse ist unerlässliche Voraussetzung für eine Internetverbindung ist, so dass deren Entstehen und Verarbeiten zwar erforderlich ist.[706] Zu prüfen ist jedoch, für welchen Zeitraum eine solche Erforderlichkeit besteht.
Die Löschung von Daten ist dementsprechend im unmittelbaren Anschluss an die vorrangige Fragestellung zu prüfen, ob überhaupt personenbezogene Daten verarbeitet werden müssen, und zwar als weitere Alternative, um Datenvermeidung und Datensparsamkeit zu ermöglichen.[707]

So beendet die Phase des Löschens von Daten die Verarbeitung der Daten, wobei die Löschung in § 3 Abs. 4 Nr. 5 BDSG definiert ist und darunter jede Form der Unkenntlichmachung gespeicherter persönlicher Daten zu verstehen

---

[705] Siehe S. 106 ff.
[706] Siehe hierzu die Ausführungen im technischen Teil S. 21und die Ausführungen auf S. 127 ff. Vgl. außerdem zur Erforderlichkeit S. 98.
[707] Siehe ebenso Fn. 58 und Fn. 463 mit dem Verweis auf Enzmann/Scholz in: Roßnagel, Datenschutz beim Online-Einkauf, S. 84, die zunächst die Frage stellen, ob überhaupt Daten verarbeitet werden müssen und anschließend darauf verweisen, dass das Optimum der Datenvermeidung durch die Beschränkung auf die Verarbeitung anonymer oder pseudonymer Datensätze erreicht wird. Hierbei muss aber berücksichtigt werden, dass nur die vollständige Anonymisierung durch irreversible Löschung geeignet ist, den Personbezug dauerhaft zu beseitigen (siehe hierzu S. 106 ff.).

ist.[708] Die Löschung stellt eine Methode dar, um einen Personenbezug dauerhaft ausschließen und Datenvermeidung sicherstellen zu können.[709]

aaa. Tunnel-Startpunkt

(1) Personenbezogenheit einer IP-Adresse

In einem VPN fallen zwangsläufig IP-Adressen an, da dies Grundvoraussetzung der Kommunikation ist.[710]
Tunnel-Startpunkte haben mindestens dynamische IP-Adressen, können aber ebenso statische IP-Adressen aufweisen.[711] So können, wie im technischen Teil bereits dargestellt, die Rechner der Nutzer sowie die Gateways oder Router von lokalen Netzwerken Tunnel-Startpunkte darstellen.[712]
Datenschutzrechtliche Relevanz haben IP-Adressen jedoch nur dann, sofern diese personenbezogen sind.[713]
Der Personenbezug von IP-Adressen ist umstritten,[714] jedoch richtigerweise aus den folgenden Gründen insgesamt zu bejahen:

So erfolgt bei statischen IP-Adressen die Zuordnung an einen bestimmten Nutzer bzw. dessen Rechner für einen längeren Zeitraum, [715] und bei

[708] Siehe hierzu Gola/Schomerus, BDSG, § 3 BDSG Rn. 40; Schaffland/Wiltfang, BDSG, § 3 BDSG Rn. 75. Aufgrund des Löschens werden die Daten unwiderruflich so behandelt, dass eigene Daten nicht länger aus den gespeicherten Daten gewonnen werden können (vgl. ebenso Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 180/181. Aus den Ausführungen von Fechner, Medienrecht, Rn. 454, ergibt sich im Übrigen, dass Löschungspflichten (als in den Datenschutzgesetzen enthaltene Schutzvorschriften) Konkretisierungen des allgemeinen Persönlichkeitsrechts darstellen. Daraus kann ebenso gefolgert werden, dass der Einzelne einen vorrangigen Anspruch auf die Löschung von personenbezogenen Daten hat, soweit sich aus den einzelnen Datenschutzgesetzen nichts anderes ergibt. Vgl. auch Büllesbach, CR 2000, 11, 16.
[709] Siehe hierzu S. 106.
[710] Zur IP-Adresse siehe S. 21ff.
[711] Siehe oben S. 57 ff.
[712] Siehe auch Lienemann, Virtuelle Private Netzwerke, S. 34 ff.
[713] Vgl. auch § 91 Abs. 1 S. 2 TKG.
[714] Roßnagel, Datenschutz beim Online-Einkauf, S. 50; Gundermann, K&R 2000, 225 ff.; Schulz, Die Verwaltung 1999, 137, 167 ff.; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 41/42 und S. 90 ff.; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 92/93/94; Löw, Datenschutz im Internet, S. 56/58; Schaar, Datenschutz im Internet, Rn. 168 ff.; Hoeren, Grundzüge des Internetrechts, S. 260/261/262; Bäumler in: Baeriswyl/Rudin, Perspektive des Datenschutzes, S. 360; siehe auch Moos, CR 2003, 385, 387.
[715] Vgl. etwa Geis, Recht im eCommerce, S. 145; Gundermann, K&R 2000, 225, 226/227; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 92/93/94; Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 53; Holznagel, MMR 2003, 219, 221. Siehe außerdem Schmitz in:

dynamischen IP-Adressen, die bei jedem Einwahlvorgang neu vergeben werden, für einen kürzeren Zeitraum. In beiden Fällen lässt sich ein Personenbezug herstellen.

Bei dynamischen IP-Adressen wird der Personenbezogenheit regelmäßig zwar für Dritte, wie etwa Webserver-Betreiber verneint. [716] Im Hinblick auf Access-Provider wird jedoch festgestellt, dass die IP-Adresse einen Personenbezug aufweisen kann.[717]

Die Einordnung der IP-Adresse als personenbezogenes Datum im Hinblick auf einen Access-Provider ist folgerichtig, da diesem ebenso regelmäßig Name und Adresse des Nutzers bekannt sind sowie darüber hinaus dessen Benutzername bzw. Login-Name, welcher in der Logdatei des Internetzugangsknotens oder RADIUS-Servers[718] neben der IP-Adresse als Protokolldatum entsteht.[719]

Sofern die Auffassung vertreten wird, dass keine Anwendbarkeit des deutschen Datenschutzrechts für vom Ausland aus operierende Access-Provider mit deutschen Töchterunternehmen in Betracht kommt, da bei den deutschen Tochterunternehmen keine personenbezogenen Daten auf ihren Einwahlknoten gespeichert werden, muss folgendes berücksichtigt werden[720]: Sofern tatsächlich die in Deutschland stehenden Einwahlserver lediglich eine

---

Hoeren/Sieber, Teil 16.4 Rn. 53 unter Verweis in Fn. 3 auf Bizer DuD 1998, 277, 278, zu der Frage des Personenbezuges, wenn der durch die IP-Adresse identifizierte Rechner von mehreren wechselnden Personen genutzt wird.

[716] Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 52; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 91/95; Helfrich in: Hoeren/Sieber, Teil 16.1 Rn. 31, der allerdings darauf verweist, dass die Zuordnung einer IP-Adresse oder anderer technischer Merkmale indirekt geeignet sein kann, einen Personenbezug herzustellen. Siehe auch Kloepfer, Informationsrecht, § 13 Rn. 65, der die Personenbezogenheit bei dynamischer Vergabe der IP-Adressen bejaht, wenn der Diensteanbieter einen Datenabgleich mit dem Access-Provider vornimmt. Letzteres muss auch dann gelten und die Personenbezogenheit der IP-Adresse bejaht werden, sofern ein Access-Provider zugleich auch eigene Angebote auf (anderen) Servern bereithält.

[717] Geis, Recht im eCommerce, S. 145; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 98; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 93; siehe auch Hoeren, Grundzüge des Internetrechts, S. 262 und Bizer, DuD 1998, 277, 278, die darauf hinweisen, dass bei dynamischen IP-Adressen regelmäßig dann Personenbezug besteht, wenn der Access-Provider und der jeweilige Diensteanbieter zusammenwirken oder identisch sind. Außerdem Schaar, Datenschutz im Internet, Rn. 171 mit dem Hinweis, dass der Access-Provider auch bei dynamischer Vergabe der IP-Adresse die IP-Nummer einzelnen Nutzern zuordnen kann.

[718] Siehe zum Radius-Server S. 29.

[719] Köhntopp/Köhntopp, CR 2000, 248, 250. Für den E-Mail-Anbieter siehe Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 120.

[720] Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 106/107 führt aus, dass keine datenschutzrechtliche relevante Speicherung stattfindet, da die Bestandsdaten des Kunden direkt auf den Zentralspeicher des ausländischen Online-Dienstes gelangen und die deutsche Tochtergesellschaft diese nicht zur Kenntnis nimmt.

Weiterleitungsfunktion übernehmen, und zwar ohne selbst eine Logdatei zu führen, ist dieser Auffassung zuzustimmen. Aber dieser Umstand muss stets im Einzelfall geprüft werden und sollte nicht pauschal unterstellt werden, da bereits aus Gründen der Systemsicherheit oder Fehlersuche nicht vorstellbar ist, dass deutsche Einwahlserver („ganz“) ohne Logdatei auskommen.
Daher ist sowohl die statische als auch die dynamische IP-Adresse für den Access-Provider personenbezogen und nicht anonym.[721] So zeigt beispielsweise der Beschluss des Landgerichts Ulm vom 15.10.2003, dass es möglich ist, im Nachhinein durch die Speicherung der dynamischen IP-Adresse auf den einzelnen Nutzer zu schließen.[722]

(2) Anwendbarkeit des TKG

Nachdem gerade die Personenbezogenheit einer (nicht vermeidbaren) IP-Adresse festgestellt wurde, stellt sich nun die Frage nach ihrer Löschung.
§ 35 BDSG regelt zwar grundsätzlich Löschungsverpflichtungen, jedoch kommen hier die spezialgesetzlichen Regelungen der §§ 91 ff. TKG in Betracht,[723] da bei der Einordnung der Dienste festgestellt worden ist, dass es sich beim Access-Providing um einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG handelt.[724] Dies bedeutet im Übrigen, dass gemäß § 91 Abs. 1 S. 2 TKG die Regelungen der §§ 91 ff. TKG ebenso für juristische Personen gelten.

Dementsprechend ist bezüglich der Bereitstellung des Internetzugangs innerhalb eines Internet-VPN von Bedeutung, inwieweit der Provider gemäß § 96 Abs. 2 TKG zur Löschung der IP-Adressen verpflichtet ist.

[721] Vgl. aber auch Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 96, der den Personenbezug einer IP-Adresse mit der Begründung verneint, dass die IP-Adressen nach jeder Verbindung zu löschen sind. Aber richtigerweise sind die IP-Adressen nach jeder Verbindung zu löschen, gerade weil es sich um personenbezogene Daten handelt.
[722] LG Ulm, ITRB 2004, S. 56, 56. Aus den Gründen des Beschlusses ergibt sich, dass auch ein Nutzer, der sich mit einer dynamischen IP-Adresse einwählt, grundsätzlich identifizierbar ist. Zwar muss Strafverfolgung wirksam durchgeführt werden können, aber lediglich mit den seitens des Gesetzes zulässigen Mitteln und nicht auf Vorrat. Siehe hierzu auch den Hinweis von Antoine zu LG Ulm, ITRB 2004, S. 56, 56. Siehe in diesem Sinne auch Schaar, Datenschutz im Internet, Rn. 175, der darauf verweist, dass die Möglichkeit zur nachträglichen Ermittlung der Nutzer durch Zuordnung von IP-Nummern von Strafverfolgungsbehörden verstärkt in Anspruch genommen wird, so dass im Grunde kein Zweifel daran besteht, dass Daten über Internetnutzung, die zusammen mit der IP-Nummer gespeichert wurden, personenbezogen sind.
[723] Siehe S. 92 zum Exklusivitätsverhältnis zwischen BDSG und §§ 91 ff. TKG sowie TDDSG.
[724] Siehe S. 122 ff.

Nochmals ausdrücklich klarzustellen ist, dass die Anwendbarkeit von § 6 TDDSG im Hinblick auf die Frage der Löschung von IP-Adressen beim Access-Providing grundsätzlich nicht in Betracht kommt, auch wenn den Ausführungen der Verfasser Koenig/Neumann[725] oftmals entnommen wird, dass es sich bei der Vergabe einer IP-Adresse um einen Teledienst handelt.
Diese Ansicht ist oben bereits abgelehnt worden.[726] Darüber hinaus stellen die Verfasser zur Begründung lediglich fest, dass es sich bei IP-Nummern nicht um Nummern im Sinne des Telekommunikationsgesetzes handelt,[727] ohne aber daraus den Umkehrschluss zu ziehen, dass es sich bei der Vergabe einer IP-Adresse insgesamt um einen Teledienst handelt.[728]

Die Gesetzesbegründung zu § 96 Abs. 1 Nr. 1 TKG stellt nunmehr außerdem ausdrücklich klar, dass unter die Kennung des Anschlusses grundsätzlich ebenso eine IP-Adresse fallen kann.[729]

[725] Koenig/Neumann, K&R 1999, 145 ff.; siehe hierzu auch Tettenborn, MMR 1999, 516, 518, der in Fn. 35 darauf verweist, dass sich die Einstufung der Vergabe einer IP-Adresse auch mit den Kenntnissen in der Literatur deckt.
[726] Siehe S. 127 ff.
[727] Koenig/Neumann, K&R 1999, 145, 151. A.A. Holznagel, MMR 2003, 219 ff, der IP-Nummern als Nummer im Sinne von § 3 Nr. 10 TKG a.F. bewertet. Siehe zu der Frage der Einordnung der IP-Nummern als Nummern im Sinne von § 3 Nr. 10 TKG a.F. auch Ehmer in: TKG-Kommentar (2. Auflage), § 90 TKG Rn. 4; Schuster in: TKG-Kommentar (2. Auflage), § 3 TKG Rn. 13; Schäfer, CR 2002, 690, 693; Schuster/Müller, MMR-Beilage 10/2000, 1, 5; Trute in: Trute/Spoerr/Bosch, TKG-Kommentar, § 90 TKG Rn. 4; Koenig/Neumann, CR 2003, 182, 182 dort mit weiteren Nachweisen in Fn. 1.
[728] Insbesondere war Kern der Problemstellung, ob die Vergabe der IP-Adressen unter die Regelungskompetenz der Bundesnetzagentur nach § 43 TKG a.F. fällt. Die in dem Aufsatz von Koenig/Neumann vorgenommene Definition und rechtliche Einordnung des Begriffs „Nummer" sollte lediglich vermeiden, dass eine IP-Adresse im Sinne einer Rufnummer im (Sprach-) Telefonnetz gleichgesetzt wird, und damit an staatliche Regulierung gebunden ist (vgl. Koenig/Neumann, K&R 1999, 145, 149 ff.). Siehe hierzu aber ebenfalls die Ausführungen auf S. 183 ff.
[729] Siehe Begründung zum TKG-E, S. 120.

(3) Speicherung von statischen IP-Adressen zum Zwecke des Verbindungsaufbaus

Bei der statischen IP-Adresse handelt es sich um ein Verkehrsdatum[730] nach § 3 Nr. 30 TKG, wobei sich aus § 96 Abs. 2 TKG jedoch eine Ausnahme von der Löschungspflicht ergibt, da die Speicherung der statischen IP-Adresse und Zuordnung zu einer bestimmten Person oder Unternehmen über den Verbindungsvorgang hinaus für den Aufbau weiterer Verbindungen gewährleistet sein muss. Denn anders als eine dynamische IP-Adresse wird die statische IP-Adresse gerade nicht bei jedem Einwahlvorgang neu vergeben. Dementsprechend ist die statische IP-Adresse und Zuordnung zu einer bestimmten Person oder Unternehmen nach § 96 Abs. 2 TKG dann zu löschen, wenn das Vertragsverhältnis endet.

Der Provider darf also auf den Systemen, die er notwendigerweise zum Verbindungsaufbau benötigt (ggf. Internetzugangsknoten, RADIUS-Server oder sonstige zum Verbindungsaufbau notwendigen Systeme) die Zuordnung von IP-Adresse zu einer Person für die Dauer des Vertrages speichern, sofern anderenfalls die Verbindung nicht aufgebaut werden könnte. Dies muss im Einzelfall geprüft werden, beispielsweise ob zum Zwecke der Identifizierung des VPN-Auftraggebers die dauerhafte Zuordnung zwischen statischer IP-Adresse und der Person des VPN-Auftraggebers in Betracht kommen könnte. In diesem Fall muss der Provider zusätzlich prüfen, inwieweit eine Pseudonymisierung gemäß § 3 Abs. 6a BDSG oder Anonymisierung gemäß § 3 Abs. 6 BDSG bezüglich der Zuordnung in Betracht kommen kann.[731]

Es wird zwar ebenso vertreten, dass es sich bei einer statischen IP-Adresse um ein Bestandsdatum im Sinne von § 3 Nr. 3 TKG handelt.[732] Damit käme § 94 Abs. 3 TKG zur Anwendung mit der Folge, dass die IP-Adresse bzw. die Zuordnung der IP-Adresse zu einer Person erst mit Ablauf des auf die

[730] Vgl. auch Büllesbach, CR 2000, 11, 16. Im Zuge der geplanten Gesetzesnovellierung des TKG wurden geltende Begrifflichkeiten wie „Verbindungsdaten" ausgetauscht und durch „Verkehrsdaten" (siehe § 3 Nr. 30 TKG) ersetzt. Diese Begriffe sollen aber nach dem Willen der Bundesregierung gleichbedeutend sein, vgl. Fn. 28.
[731] Siehe S. 106 ff.
[732] So Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 98; Hoeren, wistra 2005, 1, 4.

Beendigung des Vertragsverhältnisses folgenden Jahres zu löschen wäre. Zu berücksichtigen ist aber, dass § 3 Nr. 3 TKG eine Datenerhebung voraussetzt, wobei sich das Merkmal des „Erhebens“ in § 3 Abs. 3 BDSG[733] findet und das Beschaffen von Daten über den Betroffenen beinhaltet. Eine solche Datenbeschaffung wird als Vorphase, d.h. Voraussetzung für die nachfolgende Verarbeitung angesehen.[734]
Geregelt wird folglich der datenschutzrechtliche Umgang mit bereits existierenden Daten über den jeweiligen Kunden,[735] wozu etwa neben Name und Anschrift dessen Rufnummer gehören kann. Dabei handelt es sich jedoch nicht um eine Rufnummer, die von der Telefongesellschaft erst noch zu vergeben ist, sondern um eine bereits verfügbare bzw. vorhandene Rufnummer. Damit ist für die Einordnung einer Telefonnummer als Bestandsdatum das jeweilige Verhältnis entscheidend. Derjenige, der seine Telefonnummer bei einer datenverarbeitenden Stelle angibt, gibt ein Bestandsdatum preis. Derjenige, der einen Telefonanschluss beantragt, bekommt jedoch seitens der Telefongesellschaft eine Telefonnummer erst noch zugeteilt, so dass es sich bei dem Vorgang der Zuteilung einer Rufnummer an den Anschlussinhaber nicht um ein Erheben von Daten im Sinne von § 3 Abs. 3 BDSG handelt. Davon unberührt bleibt natürlich die Möglichkeit, dass die Telefonnummer im Vertragsverhältnis zwischen der Telefongesellschaft und ihrem Kunden nachträglich dadurch zum Bestandsdatum wird, dass die Telefongesellschaft die (Angabe der) Rufnummer selbst für die inhaltliche Ausgestaltung oder Änderung desselben (oder anderen) Vertragsverhältnisses benötigt.

Die gleichen Grundsätze, die gerade hinsichtlich einer Telefonnummer entwickelt wurden, gelten ebenso für die Einordnung von statischen IP-Adressen. Die statische IP-Adresse kann daher ebenso erst „im Verlaufe“ der Diensterbringung zu einem Bestandsdatum werden, sofern sie für die inhaltliche Durchführung des Dienstes benötigt wird. Dies kommt beispielsweise bei einer Vertragsänderung in Betracht. Ansonsten hat aber die statische IP-Adresse

[733] Zur Anwendbarkeit des BDSG siehe oben S. 92.
[734] Gola/Schomerus, BDSG, § 3 BDSG Rn. 24.
[735] Schneider, Handbuch des EDV-Rechts, Teil B Rn. 188 verweist etwa im Zusammenhang mit dem „Beschaffen von Daten über den Betroffenen“ auf Fragebögen.

ebenso wie die dynamische IP-Adresse lediglich die Aufgabe, den Nutzungsvorgang sicherzustellen.
„Erheben" meint also insgesamt „vorhandene Daten beschaffen"[736] bzw. gewinnen und nicht „Daten erschaffen".[737]
Demgemäß handelt es sich bei der statischen IP-Adresse im Verhältnis zwischen VPN-Auftraggeber und Access-Provider, die letzterer „erst noch" vergeben muss, um ein Verkehrsdatum gemäß § 3 Nr. 30 TKG und nicht um ein Bestandsdatum. Entgegen § 3 Nr. 3 TKG, § 3 Abs. 3 BDSG muss die statische IP-Adresse nicht beschafft bzw. erfragt werden, um ein Vertragsverhältnisses über Telekommunikationsdienste begründen, inhaltlich ausgestalten, ändern oder beendigen zu können, sondern diese wird vielmehr (erst) künftig bei der Erbringung des Telekommunikationsdienstes verwendet.[738]

(4) Speicherung von dynamischen IP-Adressen für Abrechnungszwecke

Die Zuweisung dynamischer IP-Adressen als Tunnel-Startpunkt kann etwa bei kleineren Außenstellen in Betracht kommen, bei welchen sich der Kauf und Betrieb eines Gateway aus finanziellen Gründen regelmäßig nicht lohnt, oder bei einem Software-VPN.[739]

---

[736] Gola/Schomerus, BDSG, § 4 BDSG Rn. 18, wo ausgeführt ist, dass § 3 Abs. 3 BDSG das aktive Beschaffen von Daten durch Befragen, Anfordern, Anhören und Beobachten ist. Damit geht es also beim Erheben stets um „bereits Vorhandenes".
[737] Siehe Gola/Schomerus, BDSG, § 3 BDSG Rn. 24, die auch darauf verweisen, dass bei zufälligen Beobachtungen gewonnene Daten nicht „erhoben" werden. Siehe auch Schaar, Datenschutz im Internet, Rn. 190, der auf das Erfordernis eines finalen, zielgerichteten Beschaffens von personenbezogenen Daten verweist.
[738] Hier kann demgemäß der Ausnahmefall bestehen, dass Daten, ohne diese vorher erhoben zu haben, dennoch „entstehen" und späterer Verarbeitung unterliegen können. Dies ändert selbstverständlich nichts an der Tatsache, dass es sich bei der statischen IP-Adresse ähnlich der Telefonnummer dann um ein Bestandsdatum nach § 3 Nr. 3 TKG handeln kann, sofern etwa ein Dritter die Angabe der statischen IP-Adresse im Rahmen der Begründung, Ausgestaltung, etc. eines Vertragsverhältnisses über Telekommunikationsdienste mit dem VPN-Auftraggeber, oder der Provider deren Angabe im Zusammenhang mit einer anderen Vertragsgestaltung benötigt. Anders als im Hinblick auf die Vergabe einer Telefonnummer kommt allerdings im Rahmen des (einen) gleichen Vertragsverhältnisses zwischen einem Provider und seinem Kunden nur selten in Betracht, dass die IP-Adresse im Nachhinein Bestandsdatum wird, da die Telefonnummer regelmäßig benötigt wird, um den Kunden in Vertragsangelegenheiten kontaktieren zu können. Die (Angabe der) IP-Adresse wird jedoch regelmäßig nur in einem anderen bzw. weiteren Vertragsverhältnis benötigt und nicht mehr im Rahmen des Access-Providing. Siehe auch Schaar, Datenschutz im Internet, Rn. 392, der die statische IP-Adresse als Bestandsdatum einstuft, die dynamische IP-Adresse hingegen als Nutzungsdatum bewertet. Allerdings wendet Schaar hier nicht das TKG an, sondern das TDDSG.
[739] Siehe S. 57.

Von den Landgerichten Stuttgart und Hamburg wird vertreten, dass es sich bei der dynamischen IP-Adresse um ein Bestandsdatum handelt,[740] so dass auch hier die Folge wäre, dieses Datum gemäß § 95 Abs. 3 TKG längerfristig speichern zu dürfen.
Richtigerweise handelt es sich jedoch bei einer dynamischen IP-Adresse ebenso und „erst recht" um ein Verkehrsdatum gemäß § 3 Nr. 30 TKG, da es bei jedem Einwahlvorgang erneut vergeben wird.
Die Landgerichte führen zu Unrecht aus, dass bereits die dynamische IP-Adresse geeignet sei, den betreffenden Anschlussinhaber eindeutig und unverwechselbar zu individualisieren. Denn die dynamische IP-Adresse ist grundsätzlich mehreren Personen zur Nutzung zugeteilt. Eine eindeutige und unverwechselbare Individualisierung kann nur dann erfolgen, sofern zusätzliche Merkmale hinzukommen, so die Dauer und der Zeitpunkt der Nutzung.
Damit ist gerade die Individualisierung der Person untrennbar mit der Nutzung im Einzelfall verbunden, so dass keine Vergleichbarkeit mit einer Telefonnummer besteht, welche unabhängig vom Zeitpunkt der Nutzung stets fix einer Person zugewiesen ist.

Demgemäß ist die Argumentation des Landgerichts Stuttgarts, es handele sich letztendlich nur um die Herausgabe eines Bestandsdatums, nicht folgerichtig.[741]
Die Zuordnung zwischen dynamischer IP-Adresse zu einer bestimmten Person ist die Grundvoraussetzung für die Feststellung, ob dieser Kunde für einen bestimmten Zeitraum an einem Telekommunikationsvorgang beteiligt war. Es wird dementsprechend Auskunft über sein Nutzungsverhalten erteilt.
Ebenso spricht die Gesetzesbegründung zu § 96 Abs. 1 Nr. 1 TKG dafür, dass es sich bei der dynamischen IP-Adresse um ein Verkehrsdatum, also um ein Datum der Nutzung, handelt. Sofern diesem Nutzungsdatum „dynamische IP-Adresse" darüber hinaus der Name einer Person zugeordnet wird, so kann nichts anderes gelten.
*Ein wesentliches Argument f*ür die ger*ade genannte Auffassung ist* außerdem, dass es sich bei der Zuordnung zwischen dynamischer IP-Adresse und einem bestimmten User um Logdateien einer Internetnutzung handelt. Logdateien

[740] LG Stuttgart NJW 2005, 614 ff.; LG Hamburg CR 2005, 833 ff.
In diesem Sinne ebenso Sankol, MMR 2006, 361 ff.
[741] LG Stuttgart NJW 2005, 614 ff. In diesem Sinne hat ebenso das LG Hamburg entschieden (LG Hamburg CR 2005, S. 833 ff.).

fallen nach zutreffender Ansicht des Landgerichts Frankfurt[742] unter Telekommunikationsverbindungsdaten, die nur unter den Voraussetzungen der §§ 100 g, h StPO beschlagnahmt werden dürfen.[743]
Sofern also eine Beschlagnahme der Gesamtdaten „Name, Adresse, Zeitpunkt und Dauer der Internetsitzung sowie IP-Adresse“ einen Richtervorbehalt benötigt, ist nicht nachvollziehbar, aus welchem Grunde die Bekanntgabe eines wesentlichen Merkmals dieses Gesamtdatenbestandes, nämlich Name und Adresse des Nutzers, ein Bestandsdatum darstellen soll. Etwas anderes ergibt sich ebenso wenig aus der Entscheidung des Bundesverfassungsgerichts vom 02.03.2006.[744] Gegenstand dieser Entscheidung war, ob die in den Endgeräten einer Telekommunikation gespeicherten Verbindungsdaten dem grundrechtlich geschützten Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG unterliegen, sofern durch eine Untersuchungsanordnung auf diese Daten in einer Privatwohnung zugegriffen wird. Dies hat das Bundesverfassungsgericht mit der Begründung verneint, dass in diesen Fällen nicht (mehr) das Fernmeldegeheimnis sondern vielmehr das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG betroffen sei.[745] Das Bundesverfassungsgericht hat weiterhin festgestellt, dass der Schutz des Fernmeldegeheimnisses zu dem Zeitpunkt ende, in welchem der Übertragungsvorgang abgeschlossen und die Nachricht beim Empfänger angekommen sei.[746]
Dies bedeutet aber im Umkehrschluss, dass Verbindungsdaten „bei“ der Übertragung (noch) vorliegen, so dass sich keine andere Bewertung des Sachverhalts ergibt.
Insgesamt muss daher in einer Gesamtschau innerhalb der jeweiligen relevanten Fallgestaltung ermittelt werden, welche Folgen die Bekanntgabe des Namens zu einer bestimmten dynamischen IP-Adresse hat. Folge einer solchen Benennung ist die Bestimmung des Nutzungsverhaltens und nicht die

---

[742] LG Frankfurt Beschluss vom 21.10.2003, 5/8 Qs 26/0.
[743] Vgl. zu §§ 100 g, h StPO als Einschränkung des Fernmeldegeheimnisses: K. Lau in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 88 TKG(2004), Band 2, Rn. 62 ff., die darauf verweist, dass es sich bei diesen Regelungen neben den Überwachungsmaßnahmen nach §§ 100 a, b StPO um weitere Ermittlungsmöglichkeiten handelt.
[744] BVerfG NJW 2006, S. 976 ff. Siehe zum Schutzumfang des Fernmeldegeheimnisses auch Eckhardt, DuD 2006, S. 365 ff., insbesondere auf S. 367 die Kritik, dass keine eindeutige Klarstellung erfolgt ist, dass die Bestimmungen des §§ 100 g, h StPO nicht durch eine Beschlagnahme beim Kommunikationsteilnehmer umgangen werden dürfen.
[745] Siehe ebenso BVerfG CR 2006, S. 383, 385.
[746] Siehe ebenso BVerfG CR 2006, S. 383, 385.

Feststellung eines Bestandsdatums, welches für die Begründung oder Änderung eines Vertragsverhältnisses notwendig wäre.

Damit handelt es sich bei einer dynamischen IP-Adresse insgesamt um ein Verkehrsdatum gemäß § 3 Nr. 30 TKG.[747] Diese IP-Adresse müsste der Provider gemäß § 96 Abs. 2, § 97 Abs. 3 TKG unverzüglich zu löschen, es sei denn sie wäre für Abrechnungszwecke erforderlich.
In dieser Frage liegt zurzeit ein besonderer Streitpunkt.

Die Erforderlichkeit der Speicherung der IP-Adresse zu Abrechnungszwecken ist vom LG Darmstadt in seiner Entscheidung vom 25.01.2006 als „nicht nachvollziehbar" verneint worden, und es hat den Provider zur unverzüglichen Löschung der IP-Adressen nach Ende eines Verbindungsvorgangs gemäß § 96 Abs.2 TKG verpflichtet.[748] Besonders bemerkenswert ist in diesem Zusammenhang, dass gemäß der obigen Ausführungen die Gerichte in Deutschland bei einer dynamischen IP-Adresse einerseits von einem Bestandsdatum ausgehen. Damit wäre zwangsläufig das Recht der Provider verbunden, die IP-Adresse gemäß § 95 TKG langfristig bzw. für die Dauer des Vertrages speichern zu dürfen. Andererseits ordnet das LG Darmstadt die IP-Adresse als Verkehrsdatum gemäß § 3 Nr. 30 TKG ein und verlangt die unverzügliche Löschung. Dieser Widerspruch zwischen den Strafgerichten und Zivilgerichten sollte im Sinne einer einheitlichen Rechtsauslegung und Rechtssicherheit für die Provider aufgelöst werden. Dies kann aber allein durch einheitliche Rechtsanwendung durch die Gerichte erfolgen, wobei das LG Darmstadt in seiner ablehnenden Entscheidung auf die Ausführungen des Bundesbeauftragten für Datenschutz verwiesen und ausgeführt hat, dass eine

[747] Ebenso Bär, MMR 2002, 358, 360; Gnirck/Lichtenberg, DuD 2004, 598, 600; Hoeren, wistra 2005, 1, 4. Gleiches ergibt sich z.B. auch aus dem Beschluss des LG Bonn vom 21.05.2004 (31 Qs 65/04) – DuD 2004, 638 ff., dem Beschluss des LG Braunschweig vom 21.03.2005 (6 Qs 100/05), dem Beschluss des LG Hannover vom 18.08.2004 (46 QS 138/04) sowie dem Beschluss des LG Memmingen vom 11.10.2004 (2 Qs 173/04).

[748] LG Darmstadt CR 2006, S. 249/250 (siehe auch die Entscheidung der 1. Instanz AG Darmstadt CR 2006, S. 38 ff. sowie der Beschluss des BGH vom 26.10.2006 (III ZR 40/06), der die Beschwerde des beklagten Providers gegen die Nichtzulassung der Revision in dem Urteil des LG Darmstadt vom 25.01.2006 wegen Nichterreichung des notwendigen Streitwerts als unzulässig verworfen hat). Siehe außerdem Dix/Schaar in: Roßnagel, Recht der Multimedia-Dienste, § 6 TDDSG Rn. 157, die darüber hinaus beim Access-Providing von einem Teledienst ausgehen. A.A. Wittern in: TKG-Kommentar (3. Auflage), § 97 TKG Rn. 5, der die Speicherung der IP-Adresse auch bei einer Flatrate für erforderlich hält.

Zuordnung der Verkehrsdaten zum Kunden auch über den Benutzernamen (so genannte. Nutzer-ID) oder die Telefonnummer erfolgen könne.
Diese Einschätzung ist insoweit zwar richtig. Allerdings wird dabei verkannt, dass dadurch auf den Abrechnungssystemen der Provider ein personenbezogenes Datum (IP-Adresse) lediglich durch ein anderes (Nutzer-ID) ausgetauscht wird. Daher ist nicht erkennbar ist, wo im Sinne einer effektiven Datenvermeidung gemäß § 3a BDSG der datenschutzrechtliche Vorteil liegt. Tatsache ist, dass im Rahmen von Telekommunikationsvorgängen (irgend)ein Identifizierungsmerkmal für die Abrechnung erforderlich ist. Sofern ein Abrechnungssystem auf der Verwendung einer IP-Adresse (als Identifizierungsmerkmal) basiert, ist nicht nachvollziehbar, aus welchem Grund diese Systeme nun umgebaut werden müssen und die Benutzerkennung als Basis der Abrechnung genommen werden sollte. Dies würde lediglich eine Verschiebung der Anknüpfungspunkte darstellen. Lediglich wenn beide Identifizierungsmerkmale (IP-Adresse und Nutzerkennung) tatsächlich im Rahmen des Übertragungsvorgangs auf den Abrechnungssystemen anfallen, ist eines von beiden aus Gründen der Datensparsamkeit und Datenvermeidung gemäß § 3a BDSG zu löschen. Da jedoch nicht ersichtlich ist, dass das TKG der Benutzerkennung gegenüber der IP-Adresse den Vorzug eingeräumt hätte, muss der Provider entscheiden können, welches Merkmal er zur Abrechnung verwenden möchte.

Außerdem ist zu berücksichtigen, dass eine IP-Adresse nur nach erfolgter Authentifizierung als letzter Schritt im Einwahlprozess vergeben wird und jede zusätzliche Einwahl über dieselbe Nutzerkennung eine andere IP-Adresse erhält. Die Speicherung der IP-Adresse ist eine Möglichkeit, um unterschiedliche Nutzungsvorgänge zu differenzieren und eine Parallelnutzung aufzeigen zu können. Dies gilt etwa bei zeitgleichem Aufbau von alternativen Verbindungen durch Verwendung der gleichen Benutzerkennung, die jedoch nicht vom Nutzungsumfang einer Flatrate abgedeckt sind.[749] So ist der

[749] Vgl. hierzu auch Moos, CR 2003, 385, 386/387, der die Auffassung vertritt, dass von der Speicherung gemäß § 7 Abs. 3 TDSV (nunmehr § 97 Abs. 3 TKG) ebenso die Möglichkeit gedeckt ist, die dynamische IP-Adresse zu speichern, um nachzuvollziehen, ob und in welchem Umfang nicht von einer Flatrate abgedeckte Nutzungen erfolgt sind (etwa Nutzungen durch den zeitgleichen Aufbau alternativer Verbindungen oder Internet-Verbindungen von Mitbenutzern des Flatrate-Kunden).

Internetzugang auf mehrere Arten möglich. Der Nutzer kann sich von zu Hause einwählen, per Laptop vom Ausland, per Handy, DSL, etc. Insoweit besteht eine Überschneidung zu den Betrugsfällen gemäß § 100 Abs. 3 TKG, die im nachfolgenden Punkt behandelt werden.

Aus rechtspolitischer Sicht ist darüber hinaus nicht zu unterschätzen, welche Bedeutung einer unverzüglichen Löschungsfrist von IP-Adressen zukommt. Ohne IP-Adressen wäre die Strafverfolgung von Straftaten im Internet in erheblichem Maße erschwert. So besteht also hier die Gefahr, dass durch unverzügliche Löschungsverpflichtungen im Hinblick auf IP-Adressen eine (gesetzliche Verpflichtung zur) Vorratsdatenspeicherung gerade forciert wird. Über eine solche gibt es seit dem 11. September 2001 eine europaweite Diskussion. Ein entsprechender Gesetzesentwurf hat bislang keine Umsetzung erfahren.[750] Jedoch gibt es eine weitere EU-Richtlinie zur Vorratsdatenspeicherung, die von den EU-Justizministern am 21.02.2006 beschlossen wurde.[751] Die Mitgliedstaaten verpflichten sich darin, den Telekommunikationsdiensteanbietern eine Speicherungsfrist von mindestens

[750] Vgl. Entwurf eines Gesetzes zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen, Bundestag-Drucksache 14/9801, S. 7 ff. Der Gesetzesentwurf sah eine Ergänzung des TDDSG und des TKG dahingehend vor, dass in einem neu einzufügenden § 6a TDDSG und in Abänderung des § 89 Abs. 1 S. 1 und S. 3 TKG a.F. die Vorratsdatenspeicherung für Zwecke der Strafverfolgung und der Gefahrenabwehr als zulässig einzustufen ist. In diesem Sinne sollten vor allem Mindestfristen für die Speicherung von Bestands-, Nutzungs- und Abrechungsdaten festgelegt werden (siehe Bundestag-Drucksache 14/9801, S. 8). Dieser Vorschlag ist jedoch mit der Begründung abgelehnt worden, dass eine präventive generelle Speicherung von Nutzungs- und Abrechnungsdaten verbunden mit Bestandsdaten die Bildung von Persönlichkeitsprofilen erheblichen Ausmaßes zulassen würde (siehe Bundestag-Drucksache 14/9801, S. 15). Außerdem muss berücksichtigt werden, dass im Einzelfall mit einer solch umfassenden Speicherung ein erheblicher Grundrechtseingriff verbunden sein kann (siehe Bundestag-Drucksache 14/9801, S. 16). Vgl. aber zur zulässigen Speicherung über zukünftig entstehende Daten, unter anderem gemäß § 100g, § 100h StPO, Eckhardt, DuD 2002, 197, 200 sowie Bizer, DuD 2002, 237, 237.

[751] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. EG Nr. L 105 vom 13.04.2006, S. 54). Siehe hierzu auch Spindler/Dorschel, CR 2006, 341, 344; Büllingen, DuD, 349, 350. Siehe zu den Auswirkungen einer Vorratsdatenspeicherung auch Köcher/Kaufmann, DuD 2006, 360, 364. Vgl. außerdem dem die Pressemitteilung des Bundesjustizministeriums, abrufbar unter http://www.bmj.bund.de/enid/0,0/Presse/Pressemitteilungen_58.html? (Website vom 09.11.2006), in der unter Punkt 4 darauf verwiesen ist, dass aus dem Bereich des Internets nur Daten über den Internetzugang sowie über E-Mail-Kommunikation und Internettelefonie erfasst sind. Kommunikationsinhalte dürfen zwar nicht gespeichert werden. Allerdings müssen die genannten Daten – anders als in der Regel nach geltendem Recht – auch dann gespeichert werden, wenn sie nicht für die Gebührenabrechnung benötigt werden, wie dies bei Pauschaltarifen (Flatrates) der Fall ist

sechs Monaten für im Einzelnen aufgeführte Telekommunikationsbestands- und –verkehrsdaten aufzuerlegen. Den Mitgliedstaaten steht es frei, diese Frist im nationalen Recht bis auf 24 Monate auszudehnen. Zweck der Speicherung ist die Ermittlung, Aufdeckung und Verfolgung schwerer Straftaten, zu denen auch alle mittels Telekommunikation begangenen Straftaten gehören.

Zur Vermeidung solcher gesetzlichen Mindestspeicherungsfristen von 12 oder 24 Monaten, die dem Grundsatz der Datensparsamkeit und Datenvermeidung gerade zuwiderlaufen, sollte sich in rechtspolitischer Hinsicht die Frage daher letztendlich darauf beziehen, für welchen Zeitraum eine Speicherung von IP-Adresse angemessen, erforderlich und datenschutzfreundlich ist.
§ 97 Abs. 3 geht von einer Höchstspeicherungsfrist von sechs Monaten aus. Im Falle einer monatlichen Abrechnung ist dieser Zeitraum allerdings nur vertretbar, sofern der Kunde tatsächlich Einwendungen gegen die Rechnung vorbringt. In diesen Fällen darf der Provider die Daten auch länger als sechs Monate speichern.[752]
Insgesamt bietet sich bei der Beurteilung darüber hinaus eine Parallele zu der Speicherungsfrist der TDSV1996 an, nach welcher der Diensteanbieter gemäß § 6 Abs. 3 TDSV 80 Tage Zeit hatte, um die Abrechnung vorzunehmen. Dieser Zeitraum liegt im ebenso Interesse des Kunden, da er in dieser Zeit auch eigene Bedenken gegen die Abrechnung anmelden kann. So hatte dieser Zeitraum ursprünglich den Sinn, den Kundenschutz sicherzustellen, da der Kunde auf diese Weise noch ausreichend Zeit hatte, um die Rechnungsposten zu reklamieren.

Aufgrund der Regelung des § 97 Abs. 3 TKG kann die Einführung gesetzlicher Mindestspeicherungsfristen daher unterbleiben.[753] Überschreitet ein Provider im Sinne eines wirksamen und verantwortungsbewussten Datenschutzes diese Höchstdauer nicht und löscht IP-Adressen nach einer kurzen Frist, so ist dadurch mehr Datenschutz „gewonnen“ als wenn gesetzliche Mindestspeicherungsfristen eingeführt werden. Diese führen letztendlich zu einer staatlich vorgegebenen Vorratsdatenspeicherung und widersprechen dem

[752] Vgl. Königshofen/Ulmer, Datenschutz-Handbuch Telekommunikation, § 97 TKG Rn. 14.
[753] Siehe zur allgemeinen Grenze für die Dauer der Speicherung für entgeltrelevante Daten auch Klesczewski in: Berliner Kommentar zum TKG, § 96 TKG Rn. 14.

Grundsatz der Datenvermeidung. Insbesondere führt dies zu einer staatlichen angeordneten Überwachung der Bürger, die durch eigenverantwortliches und datenschutzgerechtes Handeln der Provider vermieden werden könnte.

(4) Speicherung von dynamischen IP-Adressen zur Aufdeckung von Missbrauchsfällen

Eine Ausnahme von der Löschungspflicht der dynamischen IP-Adresse als Tunnel-Startpunkt kann sich des Weiteren aus § 100 Abs. 3 TKG ergeben.[754] Ein Diensteanbieter darf gemäß § 100 Abs. 3 TKG bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte die Bestandsdaten und Verkehrsdaten erheben und verwenden, die zum Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste erforderlich sind.
Wie sich allerdings aus dem Wortlaut von § 100 Abs. 3 TKG ergibt, müssen tatsächliche Anhaltspunkte für eine rechtswidrige Inanspruchnahme *seines eigenen* Dienstes vorliegen. Damit bezieht sich dieser Tatbestand ausschließlich auf den Missbrauch der Dienstleistung des Anbieters eines Telekommunikationsdienstes, insbesondere eines Access-Providers, und nicht auf den Missbrauch von Diensten Dritter, etwa fremder Websites.

Dennoch wird die Anwendbarkeit von § 100 Abs. 3 TKG ebenso bei Missbrauch von Diensten Dritter teilweise bejaht. So wird als Hauptargument für die Legitimation der Speicherung die Systemsicherheit der Online-Angebote angeführt,[755] da sich im alltäglichen Betrieb der Website mit monatlichem millionenfachen Zugriff Störungen durch technische Umstände, Fehlbedienungen oder vorsätzliche Handlungen ergäben, welche sich nur durch Auswerten von Logdateien effektiv analysieren und korrigieren lassen.[756]

---

[754] Siehe zur Missbrauchsbekämpfung gemäß § 100 Abs. 3 TKG Klesczewski in: Berliner Kommentar zum TKG, § 100 TKG Rn. 14 ff.
[755] Heidrich, DuD 2003, 237, 238.
[756] Heidrich, DuD 2003, 237, 238.

Ein solcher Missbrauch von Websites (Dritter) ließe sich jedoch nur aufdecken, sofern entweder der Website-Betreiber entsprechende Log-Files[757] erstellt und diese mit den Daten des Access-Providers zusammenführt,[758] oder aber durch die Speicherung und Verknüpfung von IP-Adressen[759] und aufgerufenen Websites seitens des Access-Providers.
Dies geht aber, wie gerade ausgeführt, über den Anwendungsbereich dieser Vorschrift hinaus, so dass eine Speicherung der Daten zu diesem Zweck unzulässig wäre.

Für eigene Zwecke, etwa Betrugsfälle, die darin bestehen, die elektronischen Kommunikationsdienste ohne entsprechende Bezahlung zu nutzen,[760] darf der Provider jedoch gemäß § 100 Abs. 3 TKG aus allen Verkehrsdaten, die nicht älter als sechs Monate sind, die Daten der Verbindung des Netzes ermitteln, aus denen sich tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme von TK-Netzen und –Diensten ergeben.
Der Provider darf insbesondere einen Gesamtdatenbestand aus Verkehrsdaten und pseudonymisierten Bestandsdaten bilden (§ 100 Abs. 3 S. 3 TKG).[761]

---

[757] Auch auf dem Web-Server wird die Anfrage des Nutzers in einer Logdatei gespeichert, wobei unter anderem die IP-Adresse des anfragenden Client von der Speicherung umfasst ist (vgl. auch Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 48/82 mit dem Hinweis, dass Website-Anbieter häufig Protokolldaten über den Ablauf der Nutzung in so genannten Log-Files speichern.). Siehe außerdem zu Log-Files und der Speicherung der IP-Adresse auf dem Server des Website-Inhabers: Roßnagel, Datenschutz beim Online-Einkauf, S. 41; Köhntopp/Köhntopp, CR 2000, 248, 251 sowie Cichon, Internetverträge (1. Auflage), S. 71, letztere mit Ausführungen im Hinblick auf die Erstellung von Statistiken des Providers über Häufigkeit, Dichte und Tageszeiten des Zugriffs auf die Webseiten und zwar auch unter Speicherung der Herkunfts-IP-Adresse der Besucher.
[758] Die Verknüpfung zwischen einzelner besuchter Website und IP-Adresse ist dann möglich, wenn der Website-Inhaber auf seiner Website Zugriffstatistiken hat und dadurch auch registriert wird, welche IP-Adresse die Website besucht hat und welche Daten heruntergeladen (Download) hat. Siehe auch Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 82, der darauf verweist, dass nicht nur Datum, Uhrzeit und Dauer der Internetsitzung erfasst werden, sondern die Inhaber einer Website in einem solchen Fall ohne großen Aufwand weitere Informationen ermitteln können, wie Herkunftsland des Nutzers und Internet-Domain, die seiner IP-Adresse zugeordnet ist, woraus sich wiederum der Provider ergibt, über den sich der Nutzer in das Internet eingeloggt hat.
[759] Vgl. Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 102, der darauf verweist, dass ein Vermarkter (Betreiber einer Website) aus der IP-Adresse den Access Provider ermitteln kann, und dass einige Vermarkter zu diesem Zweck Providerdatenbanken angelegt haben, in der die jeweiligen IP-Nummernräume der einzelnen Provider gespeichert sind.
[760] Siehe Erwägungsgrund 29 der EU-Richtlinie 2002/58/EG.
[761] Vgl. Ohlenburg, MMR 2004, 431, 437.

Dies bedeutet aber auch, dass der Provider die grundsätzliche Gelegenheit haben muss, den konkreten Missbrauchsverdacht von Nutzern feststellen zu können.
Würde unmittelbar nach dem Ende der Verbindung eine Löschung der IP-Adresse erfolgen, so hätte der Diensteanbieter keine Möglichkeit mehr, den Missbrauchsverdacht aufzudecken.[762] Da aber auf der anderen Seite ebenso die Vorratsdatenspeicherung vermieden werden muss, ist das sich aus § 100 Abs. 3 TKG ergebende Recht, die Daten der letzten sechs Monate herauszufiltern, einschränkend auszulegen. Der Provider muss daher diesen konkreten Missbrauchsverdacht unverzüglich, d.h. so schnell wie möglich, ermitteln.[763] Dabei sind belegbare und nachvollziehbare Gründe darzulegen.

Zuzugeben ist zwar, dass § 100 Abs. 3 TKG insoweit unklar ist, dass zwar einerseits gemäß § 100 Abs. 3 S. 1 TKG für die Verarbeitung tatsächlich zu dokumentierende Anhaltspunkte verlangt werden, aber dass andererseits der Wortlaut des § 100 Abs. 3 S. 2 TKG den Schluss nahe legen könnte, der Provider dürfte von vorneherein sämtliche Verkehrs- und Verbindungsdaten sechs Monate lang speichern, um diese dann im nachhinein bei konkretem Missbrauchsverdacht auszuwerten.
Dies ist jedoch nicht der Fall. § 96 Abs. 2 TKG ist insoweit eindeutig und legt fest, dass Daten, die nicht für die Abrechnung erforderlich sind, unverzüglich nach Verbindungsende zu löschen sind.[764]
Unverzüglich bedeutet „ohne schuldhaftes Zögern".[765] Dies kann aber nur anhand einer Einzelfallbetrachtung festgestellt werden und es sollten keine festen Löschungsfristen vorgeschrieben werden. Vielmehr sollten die Provider in einem eigenverantwortlich gestalteten Prozess nachvollziehbar darlegen, welche Fristen hier angemessen sind und wie in welchem Zeitraum die

[762] Vgl. auch Wittern in: TKG-Kommentar (3. Auflage), § 97 TKG Rn. 5 mit dem Hinweis, dass ohne das Vorhalten einer IP-Adresse ein Denial of Service Attack nicht aufgedeckt werden könne.
[763] Aus diesem Grunde ist auch nicht nachzuvollziehen ist, weshalb durch die Umsetzung der Richtlinie nun unbegrenzte Speicherung erlaubt sein solle (siehe die Auffassung von Moos CR 2003, 385, 387).
[764] Dies ist durch Artikel 6 Abs. 1 und Abs. 2 der EU-Richtlinie 2002/58/EG im Übrigen festgelegt worden.
[765] Siehe zur Unverzüglichkeit Königshofen/Ulmer, Datenschutz-Handbuch Telekommunikation, § 96 TKG Rn. 14.

„Unverzüglichkeit“ umzusetzen ist.[766] Hierbei muss der Ausgangspunkt stets der sein, die Daten „so schnell wie möglich“ zu löschen. [767]

(5) Speicherung von IP-Adressen zur Behebung von Störungen

In Bezug auf Störungen regelt § 100 Abs. 1 TKG, dass der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden darf, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen erforderlich ist.[768] Damit darf der Access-Provider grundsätzlich ebenso die IP-Adresse für diesen Zweck speichern.
Im Gegensatz zu § 9 Abs. 1 TDSV1996 ist nun aber im Rahmen von § 100 Abs. 1 TKG nicht mehr erforderlich, dass im Einzelfall tatsächlich Störungen und Fehler oder konkrete Anhaltspunkte dafür vorliegen.[769] Dies bedeutet, dass ein Provider nun vorsorglich Daten zum Zwecke der Störungsbehebung speichern darf. [770] § 100 Abs. 1 TKG enthält zwar nicht explizit eine Speicherungs(höchst)frist. Aus der Einschränkung der Erforderlichkeit ergibt sich jedoch, dass die Daten zu löschen sind, sofern diese nicht oder nicht mehr für die Störungsbeseitigung benötigt werden.[771] Die gesetzliche Definition einer konkreten Frist wäre allerdings nicht sinnvoll, da der Löschungszeitpunkt im Einzelfall unterschiedlich sein kann.[772] So können für Zwecke der Störungssuche zwar zwei Wochen ausreichend sein.[773] Aber dieser Zeitraum kann im Einzelfall ebenso länger oder kürzer sein.

---

[766] Vgl. auch Ohlenburg, MMR 2004, 431, 437.
[767] Siehe zur grundsätzlich restriktiven Auslegung des Rechts auf Protokollierung, Bizer, DuD 2006, 270, 273. Siehe zu den Vorgaben einer Speicherdauer und einer am Einzelfall orientierten Betrachtungsweise auch Schoen, DuD 2005, 84, 86 (der sich in seinen Ausführungen allerdings auf die gesetzliche Grundlage des TDDSG bezieht).
[768] Diese Regelung entspricht im Übrigen auch dem Erwägungsgrund 29 der EU-Richtlinie 2002/58/EG, wonach der Diensteanbieter Verkehrsdaten in Bezug auf Teilnehmer und Nutzer in Einzelfällen verarbeiten kann, um technische Versehen oder Fehler bei der Übertragung von Nachrichten zu ermitteln.
[769] Klesczewski in: Berliner Kommentar zum TKG, § 100 TKG Rn. 8.
[770] Klesczewski in: Berliner Kommentar zum TKG, § 100 TKG Rn. 8.
[771] Siehe zur Störungsbehebung außerdem die Ausführungen von Büchner in: TKG-Kommentar (2. Auflage), § 7 TDSV (Anh § 89 TKG) Rn. 1, der auf die durch die Grundsätze der Verhältnismäßigkeit, Erforderlichkeit und der Zweckbindung eingeschränkte Nutzungsbefugnis verweist. In diesem Sinne ebenso Wittern in: TKG-Kommentar (3. Auflage), § 100 TKG Rn. 7.

[772] Vgl. Ohlenburg, MMR 2004, 431, 437.
[773] Gerling, DuD 2005, 338, 339.

Auch hier sollten daher die Provider in einem bewussten und von eigenverantwortlichem Handeln geleiteten Datenschutz die Löschungsfristen bestimmen und in Datenschutzkonzepten festschreiben können, welche im Übrigen jederzeit von der Datenschutzaufsichtsbehörde überprüfbar wären. Der Ansatzpunkt muss dabei stets sein, dass die Datenlöschung „so schnell wie möglich“ zu erfolgen hat, so dass in die Betrachtung gleichermaßen die Kapazitäten des Providers einbezogen werden können.

bbb. Tunnel-Endpunkt

(1) Verkehrsdatum

Bei der IP-Adresse des angewählten Standortes (Ziel-IP-Adresse) handelt sich um ein Verkehrsdatum gemäß § 96 Abs. 1 Nr. 1 TKG, da diese eine Nummer des beteiligten Anschlusses darstellt.[774] Dieses Datum ist vom Provider, der dem VPN-Auftraggeber den Internetzugang bereitstellt, nach dem Ende der Verbindung gemäß § 96 Abs. 2 S. 2 TKG auf dem Internetzugangsknoten und sonstigen bei der Einwahl in das Internet verwendeten Systemen, die Logdateien führen, unverzüglich zu löschen. Sonstige bei der Internetverbindung verwendete Systeme sind etwa Radius-Server.[775]

Etwas anderes ergibt sich lediglich in den Fällen, in denen die Speicherung weiterhin für die in §§ 97, 99 und 100 TKG[776] genannten Zwecke erforderlich wäre. Regelmäßig wird die Speicherung der Ziel-IP-Adresse allerdings nicht benötigt und ist für den Access-Provider irrelevant.[777] Bei der nächsten Einwahl kann die Ziel-IP-Adresse wiederum seitens des Client angegeben und angerufen werden, ohne dass hierfür bei dem Provider eine langfristige Speicherung erforderlich ist.

[774] Robert in: TKG-Kommentar (3. Auflage), § 96 TKG Rn. 3.
[775] Siehe hierzu S. 29.
[776] § 101 TKG kann hier außer Betracht bleiben, da diese Vorschrift Regelungen bezüglich belästigender Anrufe trifft, und Anruf gemäß § 3 Nr. 1 TKG eine über einen öffentlich zugänglichen Telefondienst aufgebaute Verbindung meint, die eine zweiseitige Echtzeitkommunikation ermöglicht, wobei „öffentlich zugänglicher Telefondienst“ gemäß § 3 Nr. 17 TKG einen der Öffentlichkeit zur Verfügung stehenden Dienst für das Führen von Inlands- und Auslandsgesprächen einschließlich der Möglichkeit Notrufe abzusetzen meint.
[777] Siehe aber auch die Ausführungen auf S. 57, 146 ff. und S. 226 ff. zum zwangsweisen Tunneling.

Dies gilt sowohl für eine statische Ziel-IP-Adresse als auch für eine dynamische Ziel-IP-Adresse.[778] Zur Einsparung von Speicherplatzkapazitäten wird die Ziel-IP-Adresse im Übrigen auch ohne eine gesetzliche Verpflichtung zur unverzüglichen Löschung regelmäßig seitens der Provider gelöscht werden.

Die Ziel-IP-Adresse des angewählten Standortes ist ebenso wenig im Rahmen eines VPN (und den Provider an sämtlichen Standorten den Internetzugang bereitstellt) ein zum Aufbau weiterer Verbindungen notwendiges Verkehrsdatum nach § 3 Nr. 30 TKG, dessen Speicherung auf dem Internetzugangsknoten oder sonstiger bei der Internetverbindung verwendeten Systeme (Radius-Server) weiterhin erforderlich wäre.[779]
Der Client[780] kann in der VPN-Software oder Zugangssoftware selbst die Verbindungseinstellungen bei der nächsten Einwahl vornehmen.[781]
Insbesondere ist die IP-Adresse des angewählten Standortes für den Provider auch nicht anonym, wenn er an sämtlichen Standorten des VPN den Internetzugang bereitstellt. Die Ziel-IP-Adresse kann er eindeutig seinem Kunden bzw. dem VPN-Auftraggeber zuordnen.

Im Falle einer statischen IP-Adresse als Ziel-IP-Adresse darf der Provider diese nur speichern, wenn dieser Tunnel-Endpunkt zugleich auch Tunnel-Startpunkt ist, und er aus dem Grunde die statische IP-Adresse für den Aufbau weiterer Verbindungen benötigt.[782]
Diesbezüglich wandelt sich jedoch die Sichtweise, da sich das Speicherungsrecht nur auf den Tunnel-Startpunkt bezieht. Dies bedeutet, dass die Systeme der Datenverarbeitung unterschiedliche Voraussetzungen erfüllen müssen und bei der rechtlichen Prüfung daher auf das konkrete System abzustellen ist. Der Provider ist zur Speicherung eines Tunnel-Endpunkts nur berechtigt, wenn und weil dieser zugleich Tunnel-Startpunkt darstellt.

[778] Eine entsprechende Löschungspflicht ergibt sich im Übrigen für die dynamische IP-Adresse im Rahmen des dynamischen DNS-Server-Verfahrens (siehe hierzu S. 56). Auch diese IP-Adresse wird nicht mehr benötigt. Die Legitimation der Speicherung des Domain-Namens beim dynamischen DNS-Server-Verfahren wird an späterer Stelle behandelt (siehe S. 207 ff.).
[779] Etwas anderes kann sich im Hinblick auf das zwangsweise Tunneling ergeben (siehe hierzu die technischen Erklärungen auf S. 57 ff.), was aber erst an späterer Stelle behandelt wird (siehe S. 226 ff.).
[780] Siehe zum Client-Server-Prinzip S. 43.
[781] Siehe beispielsweise das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 72 ff.
[782] Siehe hierzu auch die Ausführungen auf S. 168 ff.

(2) Einzelverbindungsnachweis?

Gemäß § 97 Abs. 4 Nr. 1 und Nr. 2 TKG ist der Provider nach Wahl seines Kunden verpflichtet, die Zielnummer vollständig oder unter Kürzung um die letzten drei Ziffern zu speichern oder mit Versendung der Rechnung an seinen Kunden bzw. Auftraggeber vollständig zu löschen. Der Kunde kann darüber hinaus gemäß § 99 TKG diese Angaben in Form eines Einzelverbindungsnachweises verlangen.

Der Provider muss seinen Kunden auf dieses Wahlrecht hinweisen, wobei der Provider die Zielnummer ungekürzt speichern darf, sofern sein Kunde bzw. der VPN-Autraggeber von seinem Wahlrecht keinen Gebrauch macht.[783]

Da unter den Begriff „Nummer" gemäß § 3 Nr. 13 TKG ebenso eine IP-Adresse fällt,[784] liegt der Schluss nahe, dass der Provider gemäß § 97 Abs. 4 TKG

[783] Königshofen/Ulmer, § 97 TKG Rn. 12. Im Übrigen ist hier anzumerken, dass im Hinblick auf Abrechnungszwecke nach den bis zum 30.06.2004 geltenden gesetzlichen Bestimmungen der TDSV (§ 7 Abs. 3 TDSV) die Speicherung der Zielnummer für Abrechnungszwecke lediglich gekürzt um die letzten drei Ziffern möglich war. Nach § 6 Abs. 4 TDDSG hingegen dürfen und durften Nutzungsdaten (zu den Nutzungsdaten siehe S. 104 ff.) vollständig gespeichert werden. Für die Frage der Legitimation der Speicherung von IP-Adressen konnte dies insoweit Auswirkungen haben, sofern man mit der in dieser Arbeit vertretenen Meinung und der Einordnung von IP-Adressen unter das TKG, zumindest im Zusammenhang mit dem Internetzugangs-Providing, nicht folgt und IP-Adressen generell unter das TDG einordnet (siehe S. 127 ff. sowie Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, S. 149 (3. Auflage) und Tettenborn, MMR 1999, 516, 518, die die Vergabe der IP-Adressen, den DNS-Service sowie das Routing als Teledienst begreifen). Im Zuge der TKG-Novelle ist diese Frage jedoch nicht mehr relevant, da gemäß § 97 Abs. 3 TKG nunmehr ebenfalls die vollständige Speicherung möglich ist, und zwar ohne Kürzung der Zielnummer um die letzten drei Ziffern, wie es noch in § 7 Abs. 3 TDSV verlangt war. Dies würde im Übrigen wieder den Rechtszustand herzustellen, der vor der flächendeckenden Einführung von ISDN und Änderung der TDSV im Jahre 2000 herrschte. Nach § 5 Abs. 1 S. 1 Nr. 1 TDSV 1996 war die vollständige Speicherung von Ausgangsnummer und Zielnummer durch die Deutsche Telekom AG erlaubt (vgl. auch Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, S. 154 (3. Auflage)). Kubicek, CR 1990, 659, 664 verweist allerdings im Rahmen der damals geltenden Telekommunikationsordnung darauf, dass diese keine Rechtsgrundlage für die bei ISDN praktizierte Speicherung von Zielnummern bietet und bezieht sich dabei auf den 12. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, S. 39 (1986 wurde vom Bundesminister für das Post- und Fernmeldewesen auf der Grundlage der Ermächtigung durch § 14 Postverwaltungsgesetz die Telekommunikationsordnung (TKO, Verordnung über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des Fernmeldewesens (Telekommunikationsordnung – TKO) vom 05.11.1986, BGBl. I S. 1749) erlassen, die bis 30.06.1991 galt; vgl. ebenso Kubicek, CR 1990, 659, 663).

[784] Nunmehr ist in § 3 Nr. 13 TKG und § 3 Nr. 18 TKG zwischen Nummer und Rufnummer unterschieden und klargestellt wird, dass sich die Rufnummer nur auf den öffentlichen Telefondienst bezieht, also gemäß § 3 Nr. 17 TKG ein der Öffentlichkeit zur Verfügung stehender Dienst für das Führen von Inlands- und Auslandsgesprächen (vgl. auch Begründung zum TKG-E, S. 80). Eine IP-Adresse dient als Zeichenfolge hingegen der Adressierung im Internet. Außerdem ist durch die Gesetzbegründung zum TKG ausdrücklich klargestellt, dass von § 96 Abs. 1 Nr. 1 TKG ebenso die IP-Adresse erfasst sein kann. Siehe außerdem Büning/Weißenfels in: TKG-Kommentar (3. Auflage), § 66 TKG Rn. 4;

verpflichtet ist, den Kunden darüber aufzuklären, dass dieser die Möglichkeit hat, die vollständige oder gekürzte Speicherung der IP-Adresse oder aber deren sofortige Löschung zu verlangen.[785]

Im Rahmen eines VPN ist jedoch zunächst auf die Frage einzugehen, ob der Provider als Anbieter einer geschlossenen Benutzergruppe gemäß § 97 Abs. 4 S. 4 TKG von dieser Verpflichtung befreit sein könnte, sofern er an sämtlichen Standorten des VPN den Internetzugang bereitstellt[786]

Eine geschlossene Benutzergruppe ist dadurch gekennzeichnet, dass sie sich hinreichend bestimmbar von der Allgemeinheit abgrenzen lässt, und dass ihre Teilnehmer in gesellschaftsrechtlichen oder schuldrechtlichen Dauerbeziehungen oder sonstigen nicht-vertraglichen, aber dauerhaften Verbindungen zur Verfolgung gemeinsamer beruflicher, wirtschaftlicher oder hoheitlicher Ziele stehen.[787]

Aber ein Provider, der an sämtlichen Standorten eines VPN den Internetzugang bereitstellt, ist dennoch kein Anbieter einer geschlossenen Benutzergruppe. Seine Dienstleistung dient in diesem Falle ausschließlich dem Zweck, Vermittlung für Sprache für andere zu betreiben. Der gemeinsame Kommunikationszweck allein reicht jedoch nicht aus, um den Teilnehmerkreis hinreichend bestimmbar von der Allgemeinheit abzugrenzen.[788] Die in geschlossenen Benutzergruppen gebündelten Aktivitäten müssen über eine bloße Mitgliedschaft hinausgehen.[789]

Robert/Schuster/Büning/Weißenfels in: TKG-Kommentar (3. Auflage), § 3 TKG Rn. 34.. Vgl. auch S 167 ff.

[785] Im Übrigen bleibt es bei der obigen Feststellung (S. 181 ff.), dass die Ziel-IP-Adresse unverzüglich nach § 96 Abs. 2 TKG zu löschen ist, sofern es nicht um eine volumenmäßige Abrechnung handelt, wobei die der Begriff der Unverzüglichkeit auslegungsbedürftig ist.

[786] Seit der Neufassung der TDSV im Jahre 2000 ist für deren Anwendbarkeit nicht mehr erforderlich, dass Telekommunikationsdienstleistungen für die Öffentlichkeit angeboten werden. Dies bedeutet, dass hiervon ebenfalls Anbieter geschlossener Benutzergruppen erfasst werden. Vgl. noch Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 100, der darauf hinweist, dass die Anwendungsbereiche des TKG und der TDSV nicht deckungsgleich sind, da die TDSV nur für Telekommunikationsdienste gilt, die der Öffentlichkeit angeboten werden; ebenso Wuermeling/Felixberger, CR 1997, 230, 235 und Rieß, DuD 1996, 328, 329. Siehe auch Gola/Klug, Grundzüge des Datenschutzrechts, S. 198.

[787] Siehe die Ausführungen auf S. 117.Vgl. Trute/Spoerr/Bosch, TKG-Kommentar, § 3 TKG Rn. 85; siehe auch § 6 Abs. 2 Telekommunikations-Verleihungsverordnung.

[788] Vgl. Zimmer, CR 2003, 893, 894.

[789] Vgl. Moritz/Niebler, CR 1997, 697, 700; Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 100.

So können alle durch Lieferanten- oder Kundenbeziehungen verbundenen Unternehmen eine geschlossene Benutzergruppe bilden, aber nicht die Teilnehmer eines Telefonnetzes.[790]
Daraus ergibt sich, dass gegebenenfalls der Kunde des Internetzugangs-Providers gegenüber seinen Nutzern als Anbieter einer geschlossenen Benutzergruppe in Betracht kommen kann, aber niemals der (Netz- oder Internetzugangs-) Provider.[791] Denn im Verhältnis zwischen VPN-Auftraggeber und Provider stellt der Provider aus Sicht des VPN-Auftraggebers das gesamte Netz einer Allgemeinheit zur Verfügung, und zwar einer Allgemeinheit, welcher gesamtbetrachtend der gemeinsame Zweck zur Verbundenheit fehlt.
Zu berücksichtigen ist hierbei, dass das VPN lediglich ein virtuelles Netz darstellt,[792] wobei die Netzstruktur, die der Provider der Allgemeinheit zur Verfügung stellt, genutzt wird. Es ist insgesamt kein Grund ersichtlich, weshalb der Provider im Verhältnis zu den anderen Nutzern seines Netzes gegenüber dem VPN-Nutzer oder VPN-Auftraggeber privilegiert sein sollte.[793] Daher ist § 97 Abs. 4 S. 4 TKG hier nicht anwendbar, so dass der Provider an sich verpflichtet wäre, den Kunden entsprechend aufzuklären und auf dessen Wahlrecht hinzuweisen.

An dieser Stelle muss jedoch der Umstand in die Prüfung miteinbezogen werden, dass die Verkürzung der Ziel- IP-Adressen um die letzten drei Ziffern im Sinne von § 97 Abs. 4 TKG für einen Einzelverbindungsnachweis des IP-Traffic regelmäßig nicht geeignet ist.
Aus Sicht des Kunden ist ein solches Wahlrecht allenfalls im Rahmen des zwangsweisen Tunneling[794] und bei Verwendung fester IP-Adressen sinnvoll. Denn dann sind ihm die IP-Adressen auch bekannt bzw. kann er allein anhand

[790] Schütz in: TKG-Kommentar (2. Auflage), § 6 TKG Rn. 29; derselbe in: TKG-Kommentar (3. Auflage), § 6 TKG Fn. 62.
[791] Zu der Frage, ob der Kunde bzw. VPN-Auftraggeber im Verhältnis zu seinen Nutzern Telekommunikationsdiensteanbieter und Anbieter einer geschlossenen Benutzergruppe ist, siehe 302 ff. Auch in diesem Zusammenhang ist daher erforderlich, sämtliche Personenverhältnisse zu prüfen.
[792] Siehe die Ausführungen in der Einführung S. 2, wo ausgeführt worden ist, dass sich die Verbindungen eines VPN „nur wie private Leitungen darstellen".
[793] Der Provider bietet den Telekommunikationsdienst, entweder die Bereitstellung eines eigenen Backbone oder aber des Zugangs über das Internet über PoPs oder Leitungen, nicht lediglich einem (einzigen) Auftraggeber für die Einrichtung eines VPN an, sondern richtet dieses Angebot an die Öffentlichkeit. Der Provider nutzt hierbei das öffentliche Netz, wobei Öffentlichkeit ist jeder unbestimmte Personenkreis ist. Vgl. hierzu auch die Begründung zum TKG-E, S. 82. Vgl. außerdem zur Haftungsfrage § 7 TKV (zur TKV siehe Fn. 49).
[794] Siehe zum zwangsweisen Tunneling S. 57 ff.

der Speicherung der IP-Adresse nachvollziehen, wohin die Verbindung aufgebaut worden ist, was letztendlich Sinn und Zweck einer solchen Zusammenstellung der Verbindungen seitens des Providers wäre.

Problematisch wird die Nachvollziehbarkeit jedoch beim Einsatz eines dynamischen DNS-Servers[795] und beim freiwilligen Tunneling, sofern der Kunde bzw. die Nutzer ebenso die Möglichkeit haben, zu anderen (Internet-)Servern eine Verbindung aufzubauen.
Wie der Vergleich zu einer Telefonabrechnung zeigt, ist Sinn und Zweck eines Einzelverbindungsnachweises, dem Kunden zu ermöglichen, Verbindungen grundsätzlich inhaltlich nachvollziehen zu können. Dies ist bei der Auflistung von IP-Adressen in den gerade genannten Fällen nicht möglich.
IP-Adressen sind als 4-Byte-Dezimalzahl von 0 bis 255 durch je einen Punkt getrennt dargestellt (z.B. 160.149.116.8).[796] Das letzte Oktett bezeichnet den Rechner (Host-ID), die ersten Ziffern geben das jeweilige Netzwerk (Netzwerk-ID) an,[797] das dritte Oktett bezeichnet das jeweilige Subnetz.[798]
Auf den ersten Blick scheint es zwar eine brauchbare Methode zu sein, das jeweilige lokale Netzwerk im Internet[799] identifizieren zu können, sofern das letzte Oktett aus drei Ziffern besteht. Denn in diesem Falle wäre zwar nicht der einzelnen Rechner, aber zumindest das jeweilige Subnetz definiert.[800]

[795] Siehe zum Dynamic Domain Name Server auch Lipp, VPN, S. 83 sowie Voss, Das große PC & Internet Lexikon 2007, S. 290 (dynamisches DNS), insbesondere S. 56 in dieser Arbeit.
[796] Siehe zur IP-Adresse S. 35. Siehe zu diesem Beispiel außerdem das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 205.
[797] Blümel/Soldo, Internet-Praxis für Juristen, S. 28: Je nach Klasse (siehe zu den IP-Adress-Klassen A, B und C, die sich durch unterschiedliche Zahlen im ersten Oktett unterscheiden Voss, Das große PC & Internet Lexikon 2007, S. 467), wird die erste bis dritte Zahl der IP-Adresse für die Bezeichnung des Netzwerks verwandt, während die verbleibenden ein bis drei Zahlen den einzelnen Computer definieren. Siehe auch Campo/Pohlmann, Virtual Private Networks, S. 334 ff.; Davis, IPSec, S. 24 ff., die ausführen, dass die ersten Ziffern ein komplettes Netz aus verschiedenen Netzwerken bezeichnen.
[798] Vgl. die Ausführungen im Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 204.
[799] Siehe Voss, Das große PC & Internet Lexikon 2007, S. 469 mit dem Hinweis, dass es für (private) LANs drei reservierte IP-Adressbereiche gibt, unter anderem 192.168.x.x. (Klasse C), so dass auch mehrere LANs den Subnetzbereich 192.168.0.x verwenden können. Diese privaten IP-Adressen sind aber ausschließlich für die Benutzung in privaten Netzen gedacht und werden nicht von RIPE NCC vergeben und können im Internet auch nicht direkt mit anderen Netzwerken kommunizieren. Hierfür muss an der Schnittstelle zwischen einem privaten Netzwerk (Intranet) und dem Internet ein spezielles Verfahren (NAT – Network Adress Translation) eingesetzt werden, welches die private Adresse in eine öffentliche Adresse übersetzt, so dass diese für die Kommunikation im Internet auch geeignet ist (siehe Davis, IPSec, S. 28).
[800] Vgl. die Ausführungen im Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 204: Im Internet bzw. in einem Wide Area Network (WAN) können physikalisch getrennte Netzwerke (Local Area Networks –LAN) identische Netzwerknummern besitzen. Anhand dieser

Auch ist zu berücksichtigen, dass grundsätzlich die Möglichkeit gegeben ist, eine IP-Adresse ebenso einer einzigen bestimmten Person oder Organisation zuzuordnen,[801] da die Organisation „RIPE NCC“[802] an einen lokalen bzw. in Deutschland ansässigen Provider beispielsweise die Adressblöcke 195.30.0.0 bis 195.30.15.255 vergeben kann,[803] der diese wiederum an seine eigenen (und bestimmbaren) Kunden abgibt.
Jedoch ist bei Kürzung einer IP-Adresse wie beispielsweise 19530.15.25 um die letzten drei Ziffern die Bestimmung eines Subnetzbereichs nicht möglich, da sich in diesem Falle ebenso das dritte Oktett um zwei Zahlen gekürzt darstellen würde. Die gekürzte IP-Adresse könnte sich somit auf mehrere (Sub-) Netzwerke beziehen, so dass deren längerfristige Speicherung letztendlich keinen Aufschluss über die jeweiligen Verbindungen bringen würde. Auch bei entsprechender Kürzung der IP-Adresse „195.30.1.1“ wäre nur noch definiert, dass es sich um eine Adresse in einem europäischen Netzwerk handelt, und hätte insoweit keinerlei Aussagekraft.[804]

Diese Ausführungen müssen insgesamt zu dem Schluss führen, dass eine Anwendbarkeit des § 97 Abs. 4 TKG bei IP-Adressen zwar keinen Sinn macht und der Kunde durch die (zusätzliche) Speicherung der Ziel-IP-Adressen

---

Netzwerknummern kann kein Router entscheiden, ob er bei einer Kommunikation eine Verbindung zu einem anderen LAN (im Internet) aufbauen soll. Das WAN muss daher in kleine Abschnitte unterteilt werden, die einen eigenen Adressblock erhalten. Jeder Adressblock der einzelnen physikalischen Netze wird als Subnetz bezeichnet, wobei das dritte Oktett einer IP-Adresse das jeweilige Subnetz näher definiert.

[801] Siehe das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 204, wo dargestellt wird, dass diese Hierarchie (Netzwerke-Subnetze-Rechner) das Auffinden eines Rechners im Internet erleichtert, wobei der Vergleich zum Telefonnetz und der Funktion der dortigen Ortsvorwahlen gezogen wird.

[802] In Europa ist das Reseau IP European Network Control Center (RIPE NCC) mit Sitz in Amsterdam für die Vergabe und Verwaltung von IP-Nummern verantwortlich. Diese Zuständigkeit lag anfangs allein bei der Internet Assigned Numbers Authority (IANA). Verantwortlich für alle Fragen zur Organisation der Domain-Namen ist seit dem Jahre 2000 die privatrechtliche Organisation ICANN (Internet Corporation for Assigned Numbers and Names – Internetvereinigung für zugewiesene Nummern und Namen) mit Sitz in Kalifornien. ICANN ist für die weltweite Verwaltung von Domain-Namen und IP-Adressen zuständig. Sie entscheidet über technische Fragen und legt die Vergaberichtlinien von Namen und Nummern fest. Sie ist 1998 von der US-Regierung gegründet worden, trat aber erst im Oktober 2000 ihre Arbeit an und ist Nachfolger der InterNIC (Internet-Network-Information-Center) bzw. der IANA (Internet Assigned Numbers Authority), wobei die InterNIC seit 1993 im Auftrag der IANA die entsprechenden Aufgaben wahrgenommen hatte. Vgl. hierzu auch Strömer, Online-Recht, S. 9/10.

[803] Siehe zu Subnetzen und den beispielhaft genannten IP-Adressblöcken auch Davis, IPSec, S. 27.

[804] Siehe Davis, IPSec, S. 26, der unter anderem darstellt, dass die Adressblöcke 194.0.0.0 bis 195.255.255.255 für Europa zugeordnet sind (wohingegen beispielsweise 198.0.0.0 bis 199.255.255.255 sich auf den nordamerikanischen Bereich bezieht).

zudem nicht besser geschützt wäre. Nach folgerichtiger Gesetzesanwendung in dem Sinne, dass auch IP-Adressen Nummern gemäß § 3 Nr. 13 TKG darstellen wäre der Provider jedoch verpflichtet, dem Kunden die Optionen des § 97 Abs. 4 TKG anzubieten sowie gemäß § 99 TKG einen Einzelverbindungsnachweis auf Verlangen bereitzustellen. Dies könnte bei den Providern in den Praxis allerdings zu massiven Problemen führen, da Speicherkapazitäten auf den Servern oft begrenzt sind.

Eine nachvollziehbare Auflistung im Sinne eines Einzelverbindungsnachweises gemäß § 99 TKG wäre lediglich möglich, wenn der Provider anstatt der IP-Adresse den entsprechenden Domain-Namen speichert.[805] § 97 Abs. 4 TKG ist seit der Novellierung des TKG ebenso für Domain-Namen entsprechend anwendbar, da Domain-Namen ebenso Nummern im Sinne von § 3 Nr. 13 TKG darstellen.[806]

Eine Legitimation des Providers zur vollständigen Speicherung der Domain-Namen ergibt sich daher aus § 97 Abs. 4 S. 2 2. HS TKG, sofern der Provider den Kunden vorher über die Wahlmöglichkeit aufgeklärt hat, die Löschung der Domains zu verlangen.

Aber die Anwendbarkeit des § 97 Abs. 4 TKG ist insgesamt nicht nur bei IP-Adressen, sondern gleichermaßen bei Domain-Namen mit Schwierigkeiten verbunden. So besteht bei letzterem das Problem, diesen in sinnvoller Weise um die letzten drei Ziffern zu kürzen. Insbesondere stellt sich die Frage, ob damit bereits die Top-Level-Domain umfasst ist. Bei typenspezifischen Top-Level-Domains, die mindestens dreistellig sind, wäre keine wirkliche

[805] Siehe zum Einzelverbindungsnachweis Büchner in: TKG-Kommentar, § 6 TDSV (Anh § 89 TKG) Rn. 6, Wittern in: TKG-Kommentar (3. Auflage), § 99 TKG Rn. 1 ff.

[806] Siehe Büning/Weißenfels in: TKG-Kommentar (3. Auflage), § 66 TKG Rn. 4; Robert/Schuster/Büning/Weißenfels in: TKG-Kommentar (3. Auflage), § 3 TKG Rn. 34. Siehe zur gegenteiligen Auffassung, die sich allerdings noch auf die alte Gesetzesfassung stützte: Koenig/Neumann, CR 2003, S. 182 ff.; Holznagel, MMR 2003, 219, 221. Diese Auslegung ergibt sich im Übrigen nunmehr indirekt aus § 66 TKG, der zwischen Nummern und Domain-Namen ausdrücklich trennt (siehe auch Fn. 727/728). In der Begründung zum TKG-E (S. 112) ist andererseits im Hinblick auf § 66 TKG allerdings auch klargestellt, dass keine neuen Zuständigkeitsbereiche in Bezug auf die Vergabe von Namen und Adressen im Internet verbunden sein sollen, so dass sich eine eindeutige Meinung zu dieser Rechtsfrage noch herausbilden muss. Siehe zu § 43 Abs. 1 TKG a.F. und der Aufgabe der Bundesnetzagentur auch Kloepfer, Informationsrecht, § 11 Rn. 174. Vgl. außerdem Strömer, Online-Recht, S. 13 zur Frage, ob die Vergabe von Domain-Namen zu den Aufgaben der Bundesnetzagentur zählt unter Hinweis darauf, dass in diesem Falle die Bundesnetzagentur selbst die Bedingungen festlegen müsste, die zur Erlangung von Nutzungsrechten zu erfüllen sind und ein Recht auf Zuteilung begründen.

Unkenntlichmachung erreicht. Eine Verkürzung auf Second-Level-Domain-Ebene (also regelmäßig dem „eigentlichen“ Domain-Namen) wäre ebenso problematisch, sofern der Domain-Name lediglich aus drei Buchstaben besteht. Dementsprechend muss ebenso bei Domain-Namen die Feststellung getroffen werden, dass die Regelungen des Einzelverbindungsnachweises eher für den Telefonverkehr als für Internetverbindungen konzipiert sind.
Die Probleme, die sich in diesem Zusammenhang darüber hinaus im Hinblick auf die datenschutzrechtlichen Interessen des Nutzers ergeben, werden in dem Personenverhältnis „Provider/Nutzer“ dargestellt.[807]

ccc. Anschlussnummer

Der Access-Provider speichert durch die Verwendung des speziellen RADIUS-Protokolls die Anschlussnummer des Kunden.[808] Diese benötigt er auch zunächst für seine Abrechnungszwecke im Sinne von § 97 TKG, sofern er über diese Anschlussnummer den Kunden identifiziert[809] oder seine Rechnungsstellung durch den TK-Provider vornehmen lässt.
Sofern er jedoch die Identifizierung ausschließlich anhand von Nutzerdaten vornimmt, wie etwa die Vergabe eines Benutzernamens und/oder Passwortvergabe, so ist die Speicherung der Anschlussnummer nicht notwendig gemäß § 96 Abs. 2 TKG.
Dies gilt, sofern der Access-Provider die Einwahlgebühren bzw. Telefongebühren inklusive anbietet.[810] Daher muss der Access-Provider in letzteren Fällen die Anschlussnummer löschen bzw. darf sie von vorneherein aufgrund des Grundsatzes der Datenvermeidung[811] nicht speichern.

Nimmt allerdings der Access-Provider die Abrechnung seiner Gebühren über den TK-Provider vor (§ 97 Abs. 5 TKG), dann ist es seitens des Access-

[807] Siehe S. 280ff.
[808] Siehe Schaar, Datenschutz im Internet, Rn. 171, der darauf verweist, dass der Access-Provider regelmäßig die Telefonnummer durch die Verwendung des Kommunikationsprotokolls „Remote Authentication Dial In User Service“ (RADIUS) speichert.
[809] So zum Beispiel der Access-Provider MSN, der seine jeweiligen Nutzer stets über den Telefonanschluss identifiziert, an dessen Inhaber er dann die Rechnung versendet.
[810] Vgl. Kroiß/Schuhbeck, Jura online, S. 6. Siehe auch Kroiß/Schuhbeck, Jura online, S. 5, wo die Autoren darauf verweisen, dass die Gebühren sich jedoch meist auch aus den Telefonkosten zusammensetzen, die von der Telefongesellschaft erhoben werden.
[811] Siehe hierzu auch S. 15 ff. und S. 170 ff.

Providers regelmäßig erforderlich die Anschlussnummer zu speichern. Denn er muss entweder dem TK-Anbieter Name und Adresse des Nutzers oder aber die Anschlussnummer weitergeben, so dass der TK-Anbieter anhand der Telefonnummer seine Rechnungsstellung
- wie meist üblich - vornehmen kann.
In diesen Fällen ist der Access-Provider gemäß § 96 Abs. 2 TKG demnach über den Verbindungsvorgang hinaus berechtigt, die Anschlussnummer zu speichern.[812]

ddd. Standortdaten

Auch wenn der Begriff der Standortdaten insgesamt „neutral" zu betrachten ist,[813] interessieren in der Praxis hauptsächlich die exakten Lokalisierungsmöglichkeiten, wie sie im Mobilfunkbereich existieren, da diese die Erstellung eines Bewegungsprofils erlauben.

Nach § 96 Abs. 1 Nr. 1 TKG in Verbindung mit § 96 Abs. 2 TKG darf der Access-Provider Standortdaten von mobilen Anschlüssen über das Ende der Verbindung hinaus nur verwenden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, und 100 TKG genannten Zwecke erforderlich sind. Im Übrigen sind sämtliche Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.
Bei mobiler Einwahl ist die exakte Standortbestimmung -zumindest zurzeit noch – für den Access-Provider, der kein eigenes Mobilfunknetz betreibt, mit erheblichem technischem Aufwand verbunden. Dahingegen ist es jedoch für den Mobilfunkbetreiber machbar, den nahezu exakten Standort des Teilnehmers des Mobilfunknetzes zu bestimmen.[814] Zu berücksichtigen ist insbesondere, dass den meisten Nutzern eines Mobilfunknetzes eine solche Ortungsmöglichkeit nicht bewusst ist.[815]

---

[812] A.A. Dix in: Roßnagel, Recht der Multimedia-Dienste, § 5 TDDSG Rn. 33, der allerdings die übermittelte Rufnummer im Anwendungsbereich des TKG als ein Bestandsdatum einstuft und damit die Frage der Abrechnung nicht behandelt.
[813] Siehe oben S. 99 ff.
[814] Siehe hierzu Schrey/Meister, K&R 2002, 177, 184, die darauf verweisen, dass die eigene Erhebung von Standortdaten einen erheblichen technischem Aufwand bedeute, und es daher sinnvoller sei, vom Mobilfunkanbieter die Daten zur Verfügung gestellt zu bekommen.
[815] Siehe hierzu Kloepfer in: Holznagel/Nelles/Sokol, TKÜV, S. 104.

Da auch die Standortdaten zu den Verkehrsdaten zählen,[816] muss daher eine Informationspflicht des Access-Providers nach § 93 TKG dahingehend bestehen, ob er selbst in der Lage ist, Standortdaten bei mobiler Einwahl zu erheben, oder ob er solche seitens eines Mobilfunkanbieters bereit gestellt bekommt, außerdem muss er darüber informieren, für welche Zwecke und für welchen Zeitraum die Speicherung erfolgt.[817] Wichtig ist, dass dem Kunden bzw. VPN-Auftraggeber bewusst wird, dass diese Standortdaten entstehen, aber nicht unmittelbar nach Beendigung der Verbindung gelöscht werden können, und er aufgrund der Abrechnungszwecke außerdem keine Möglichkeit hat, dies zu untersagen.

Eine Löschungspflicht gemäß § 96 Abs. 2 TKG besteht nur dann nicht, sofern der Access-Provider unterschiedliche Ortstarife anbieten möchte und diese daher für seine Abrechnungszwecke benötigt, oder aber andere der in §§ 97, 99 und 100 TKG geregelten Fallgestaltungen vorliegen. Die Erhebung von detaillierten Standortdaten, die den Aufenthaltsort des Nutzers eines Mobilfunknetzes bis auf wenige Meter genau bestimmen können,[818] kann etwa bei Tarifmodellen in Betracht kommen, bei denen der Standort des VPN-Auftraggebers bei der Erbringung der Dienstleistung entgeltrelevant ist. So könnte der Access-Provider beispielsweise, ähnlich den City-Tarifen, seinen Kunden unterschiedliche Tarif- bzw. Vergütungsangebote unterbreiten.[819]

Benötigt der Access-Provider hingegen die Standortdaten für eine bedarfsgerechte Diensterbringung, so ist hierzu die Einwilligung des Teilnehmers gemäß § 96 Abs. 3 TKG erforderlich.[820] Der Begriff der „bedarfsgerechten“ Diensterbringung ist sehr umfassend und meint alle Leistungen, die Telekommunikationsdienstleistungen in ökonomischer oder

---

[816] Vgl. Erwägungsgrund 15 der EU-Richtlinie 2002/58/EG.

[817] So stellt beispielsweise AOL für verschiedene Mobilfunknetze (D1-Netz, D2-Netz und E-Plus) unterschiedliche Einwahlnummern für den mobilen Internetzugang zur Verfügung (siehe Voss, Das große PC & Internet Lexikon 2007, „AOL“ S. 74). Vgl. außerdem Artikel 6 Abs. 4 der EU-Richtlinie 2002/58/EG.

[818] Siehe S. 99 ff. sowie zu den unterschiedlichen Lokalisierungsmöglichkeiten Siehe Schrey/Meister, K&R 2002, 177, 179; Nogala/Haverkamp, DuD 2000, 31, 33; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 59; Kilian, CR 2002, 921, 921.

[819] In BfD-Info 5, Datenschutz in der Telekommunikation, 2001, S. 68, wird auf die Möglichkeit der Ortstarife bei Handygesprächen hingewiesen. Vgl. auch Schrey/Meister, K&R 2002, 177, 183, die ebenso auf diese mögliche Entgeltrelevanz eingehen.

[820] Zur Einwilligungsmöglichkeit im elektronischen Verfahren siehe § 94 TKG.

technischer Hinsicht verbessern können.[821] Bei einem VPN könnte beispielsweise die Planung und Schaffung neuer Netzkapazitäten zur bedarfsgerechten Diensterbringung zählen. Sofern der Provider in diesem Zusammenhang das standortbezogene Surfverhalten seiner Kunden auswerten möchte, benötigt er gemäß § 96 Abs. 3 TKG deren ausdrückliche Einwilligung.

Bei der Löschungsverpflichtung muss im Übrigen auch hier berücksichtigt werden, dass dem Provider aus Gründen der Abrechnung, der Systemsicherheit und zur Fehlerkontrolle das grundsätzliche Recht zur Speicherung für einen nachvollziehbaren Zeitraum zustehen muss, wobei dies ebenso belegbar dokumentiert werden muss.[822]

Ein besonderes Problem besteht in diesem Zusammenhang darin, ob für die Speicherung der Standortdaten eine Einwilligung des Kunden erforderlich ist. Diese Fragestellung ergibt sich aus dem Rechtsgedanken des § 98 TKG, der bei Diensten mit Zusatznutzen grundsätzlich eine Einwilligung des Kunden verlangt.
Dienste mit Zusatznutzen meinen jeden Dienst, der die Erhebung, Verarbeitung oder Nutzung von Verkehrsdaten oder Standortdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Entgeltabrechnung dieses Vorganges erforderliche Maß hinausgeht.[823] Die entsprechende Grundlage dieser Formulierung ist der EU-Richtlinie 2002/58/EG zu entnehmen, wobei in Erwägungsgrund 18 dieser Richtlinie beispielhaft unter anderem Navigationshilfen, Verkehrsinformationen und Wettervorhersage als Dienste mit Zusatznutzen aufgezählt werden.[824]
Die Nachrichtenübertragung beim Access-Providing findet zwar regelmäßig in Echtzeit[825] statt. Dennoch können Standortdaten im Rahmen des Internet-Access für einen längeren Zeitraum anfallen, sofern ein Nutzer „länger“ im

[821] Vgl. Robert in: TKG-Kommentar (3. Auflage), § 96 TKG Rn. 15. Siehe zur bedarfsgerechten Gestaltung von Diensten zur Erzielung ökonomisch und technisch besserer Leistungsangebote für die Zukunft Gramlich in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 89 TKG(1998), Band 1, Rn. 81.
[822] Siehe hierzu die obigen Ausführungen auf S. 177 ff.
[823] Siehe S. 102.
[824] Siehe hierzu S. 102 ff.
[825] Vgl. auch Wanckel, Persönlichkeitsschutz in der Informationsgesellschaft, S. 63, der den Begriff „Echtzeitverbindung“ verwendet und damit die Möglichkeit des unmittelbaren Datendialogs mit kurzen Antwortzeiten vorsieht.

Internet surft.. Es wäre damit grundsätzlich gerechtfertigt, hier eine Parallele zum Access-Providing zu ziehen und das Einwilligungserfordernis oder die Anonymisierungsverpflichtung ebenfalls auf die Provider auszudehnen, die Kenntnis über den Standort des jeweiligen Nutzers haben. Dennoch ist dies durch die EU-Richtlinie 2002/58/EG vollumfänglich erfasst, da ein solcher Vorgang im Sinne von Artikel 2 g) der EU-Richtlinie 2002/58/EG und § 96 Abs. 2 TKG nicht über das zur Fakturierung erforderliche Maß hinausgeht.[826]

Bei unmittelbarer Anwendbarkeit des § 98 TKG müsste der Provider seinen Kunden bzw. dem VPN-Auftraggeber außerdem die Möglichkeit gewähren, die Verarbeitung von Standortdaten zu widerrufen,[827] sofern er diese Daten noch für Abrechnungszwecke benötigen sollte.

Dementsprechend gibt es zwei Arten[828] von Standortdaten. Einerseits solche, die zwangsläufig bei der Nachrichtenübermittlung anfallen, keiner Einwilligung in ihre Verarbeitung bedürfen und nach Ende der Verbindung gemäß § 96 Abs. 2 TKG zu löschen sind.[829]

Andererseits sieht das Gesetz gemäß § 98 Abs. 1 TKG Standortdaten vor, welche „extra" für die Diensterbringung erhoben werden, um einen Dienst zu erbringen, der mit den sachlichen Verhältnissen am Standort zu tun hat bzw. bei denen die Dienstleistung nicht ohne die Standortdatenverarbeitung erbracht werden kann. Diese dürfen nur mit Einwilligung des Teilnehmers erhoben werden und für die Dauer, die der Dienst mit Zusatznutzen in Anspruch nimmt. Hierbei ist es aber unerheblich, dass Navigationshilfen[830] tatsächlich den genauen Aufenthaltsort feststellen können, wohingegen bei sonstigen Mobilgeräten regelmäßig[831] und ohne nähere Angabe des genauen

[826] Siehe zu den Tarifierungsmöglichkeiten oben S. 191.
[827] Vgl. § 96 Abs. 3, Abs. 4 TKG und § 98 Abs. 2 TKG.
[828] Siehe hierzu auch Schrey/Meister, K&R 2002, 177, 188/189, die zwar ebenfalls davon ausgehen, dass im Sinne der EU-Richtlinie 2002/58/EG zwischen zwei Arten von Standortdaten zu differenzieren ist, jedoch der Ansicht sind, dass für Standortdaten, die die Position des Nutzers genauer angeben dessen Einwilligung oder die Anonymisierung der Daten notwendig ist. Die Verfasser lassen allerdings die Frage offen, was unter „genau" zu verstehen ist. Zur Anonymisierungsmöglichkeit von Standortdaten siehe ebenso Schrey/Meister, K&R 2002, 177, 185/186.
[829] Diese Standortdaten sind identisch zu handhaben wie die übrigen in § 96 Abs. 1 TKG genannten Verkehrsdaten.
[830] Als Beispiel für den Dienst mit Zusatznutzen werden etwa Navigationshilfen genannt (siehe Erwägungsgrund 18 der EU-Richtlinie 2002/58/Eg). Hierfür wird aber das satellitengestützte Ortungssystem GPS genutzt, welches den Aufenthaltsort des Nutzers bis auf wenige Meter genau ermitteln kann (siehe Schrey/Meister, K&R 2002, 177, 179).
[831] Es kommt jedoch stets auf die Umstände des Einzelfalls an, siehe Fn. 440/441.

Aufenthaltsorts nur bestimmt werden kann, wo sich die Empfangsstation befindet. [832]

Ein Access-Provider darf also nach der jetzigen Gesetzeslage ohne Einwilligung des VPN-Auftraggebers oder Anonymisierung von dessen Daten „einfache“[833] Standortdaten verarbeiten, aber im Sinne von § 96 Abs. 2 TKG nur für die Dauer der Verbindung. Dies ergibt sich ebenso aus § 96 Abs. 1 Nr. 1 TKG.

Die EU-Richtlinie 2002/58/EG und ihre Umsetzung in § 98 TKG geht folglich offensichtlich davon aus, dass Standortdaten im Rahmen von Diensten mit Zusatznutzen (also Dienste, die eine zeitlich längere Periode in Anspruch nehmen als für die Übertragung einer Nachricht notwendig ist)[834] eine besondere „Gefährlichkeit“ bezogen auf den Datenschutz anhaften, und daher die entsprechende Aufklärung und Einwilligung des Teilnehmers und Nutzers erforderlich ist, wenn diese über einen längeren Zeitraum, und zwar den der notwendigen Nutzung hinaus, verarbeitet werden.[835]

Diese Unterscheidung ist bei näherer Betrachtung allerdings nicht gerechtfertigt, da bei jedweden Online-Vorgängen, und zwar auch bei einer Einwahl ins Internet, detaillierte Standortdaten anfallen können, und der Kunde ebenso jederzeit ortbar wäre.

Dies ergibt sich aus dem Sinn und Zweck der separaten Einwilligungsmöglichkeit bei einem Dienst mit Zusatznutzen. Dieser kann allein

[832] Siehe hierzu auch Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 106, der darlegt, dass der Aufenthaltsort sich in einer funkstreckennahen Entfernung von der bestimmten Empfangsstation befindet, aber nicht näher definiert werden kann. Siehe zur Ortung eines Mobilgeräts auch Federrath/Thees, DuD 1995, 338 ff. (die nach Lösungsmöglichkeiten und Verfahren suchen, welche die Gewinnung von Richtfunkinformationen aus elektromagnetischen Wellen stark erschweren oder unmöglich machen); siehe außerdem Beheim, DuD 1994, 327 ff. (der sich in seinen Ausführungen mit dem paneuropäischen Mobilfunkstandard GSM (Global System for Mobile Communications) beschäftigt. Wenzel, RDV 1996, S. 10, 11 nimmt auf die Gefahr des „gläsernen“ Bürgers im Zusammenhang mit der Möglichkeit des Erstellens von Bewegungsprofilen bei der Benutzung von Mobilfunk Bezug.

[833] Damit sind Standortdaten gemeint, die nicht für einen Dienst mit Zusatznutzen verarbeitet werden sollen.

[834] Vgl. Artikel 2 g) der EU-Richtlinie 2002/58/EG.

[835] Dies ist bei den neu geschaffenen Diensten mit Zusatznutzen gemäß Artikel 2 g) der EU-Richtlinie 2002/58/EG der Fall sowie in den Fällen, in welchen die Verwendung nicht durch die in § 96 Abs. 2 TKG aufgelisteten Zwecke, wie etwa Zwecke der Entgeltberechnung, Störung oder Missbrauch, gedeckt ist (siehe Erwägungsgrund 18 der EU-Richtlinie 2002/58/EG). So können beispielsweise mobile Navigationshilfen die Gefahr beinhalten, dass aufgrund eines länger andauernden Online-Vorganges der Nutzer jederzeit geortet werden kann. Die jederzeitige Ortung ist jedoch für die Entgeltberechnung nicht notwendig.

der Charakter einer Warnfunktion[836] dahingehend zukommen, dem Kunden bzw. Nutzer die stetige Möglichkeit seiner Ortung deutlich zu machen. Die Einwilligung kann aber nicht die Aufgabe haben, den Nutzer vor ungebetenen inhaltlichen (werblichen) Angeboten zu schützen.[837]

Daher wäre in rechtspolitischer Hinsicht eine Verpflichtung des Access-Providers gerechtfertigt, nicht nur gemäß § 93 TKG über die Standortdatenverarbeitung zu unterrichten,[838] sondern ebenso entsprechend § 98 TKG eine Einwilligung seitens des Teilnehmers einzuholen oder aber für die Anonymisierung dieser Daten zu sorgen, und zwar insbesondere auch dann, wenn die Standortdatenverarbeitung grundsätzlich nicht über das Ermitteln einer Nachricht und der Entgeltabrechnung hinausgeht.[839]
Die gesetzliche Vorgabe hat auf eine solche Verpflichtung jedoch verzichtet.

---

[836] Siehe zur informierten Einwilligung Wedde, DuD 2004, 169, 172, der darauf verweist, dass eine wirksame Einwilligung auf der Basis ausreichender Kenntnis der Sachlage und der Konsequenz des eigenen Handelns erfolgen muss.

[837] Denn zu beachten ist, dass die Datenverarbeitung für andere Zwecke ohnehin von der Einwilligung des Nutzers abhängig ist, vgl. auch § 93 TKG und § 96 Abs. 2 TKG, außerdem Schrey/Meister, K&R 2002, 177, 185 mit dem Hinweis, dass eine Weitergabe der Daten an Dritte nicht zulässig ist, es sei denn der Nutzer hätte eingewilligt.

[838] Siehe zur Unterrichtungspflicht bezüglich der Verarbeitung von Standortdaten ebenso die Begründung zum TKG-E, S. 120.

[839] Eine solche ausdrückliche Einwilligung und Aufklärung entspricht auch dem Erwägungsgrund 26 EU-Richtlinie 2002/58/EG, wonach Diensteanbieter die Teilnehmer stets darüber informieren sollen, welche Arten von Daten sie verarbeiten und für welche Zwecke und wie lange dies geschieht.

bb. Technische Schutzmaßnahmen

aaa. Unterrichtungspflichten über Netzsicherheit

Einem Access-Provider ist es grundsätzlich nicht möglich, eine Verschlüsselung von Nachrichten vom einzelnen Rechner bis hin zum Empfänger sicherzustellen (Ende-zu-Ende), da dies eine Aufgabe darstellt, die seitens des einzelnen Teilnehmers bzw. Nutzers zu erfüllen ist.[840]
So gibt es beispielsweise Verschlüsselungsprotokolle wie Secure Socket Layer (SSL), die regelmäßig im Internet eingesetzt werden, um Bestellvorgänge oder Online-Banking zu sichern.[841] SSL ist als Stand der Technik anzusehen,[842] insbesondere, da dieses Protokoll mittlerweile in der Software der gängigen Browser integriert ist.[843] Dies stellt jedoch eine Verschlüsselungstechnik dar, die zwischen einem Nutzer und einem Diensteanbieter eingesetzt wird, auf dessen Website der Nutzer zugreift, wie beispielsweise beim gerade erwähnten Online-Einkauf. Die Auffassung, dass Internetdienstleister nach der Telekommunikations-Datenschutzrichtlinie, die von der Richtlinie 2002/58/EG abgelöst worden ist,[844] verpflichtet sind, auch verschlüsselte Verbindungen

---

[840] Zur Verschlüsselungsmöglichkeit des Mobilfunknetzes über den GSM (Global System for Mobile Communications)- Standard siehe Beheim, DuD 1994, 327 ff., der aber darauf verweist (Beheim, DuD 1994, 327, 330), dass die Verschlüsselung nur auf der Funkstrecke zwischen Mobilgerät und einer Basisstation des Anbieters (die auf „der anderen Seite" für die Verschlüsselung verantwortlich ist) erfolgt, die Übertragung der Sprach- oder Nachrichtendaten auf Festnetzleitungen vom Netz aus unverschlüsselt geschieht. Für eine Ende-zu-Ende-Verschlüsselung ist der Mobilfunkanwender selbst verantwortlich (Beheim aaO). Siehe hierzu auch die Ausführungen des Bundesbeauftragten für den Datenschutz „Begründung zum Entwurf einer Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV), abrufbar unter www.bfd.bund.de/information/symp2_ulrich3.html (Website vom 01.08.2004). In seiner Begründung zu § 8 TKÜV legt der Bundesbeauftragte für den Datenschutz dar, dass die netzseitige Bereitstellung von Verschlüsselung nach dem heutigen Stand der Technik nur für Mobilfunknetze nach dem GSM-Standard möglich ist.
[841] Siehe Voss, Das große PC & Internet Lexikon 2007, S. 756, der die Funktionsweise von SSL erklärt.
[842] Koenig/Röder, CR 2000, 668, 671.
[843] Siehe Schaar in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 399, der ebenfalls darauf verweist, dass SSL der Absicherung zwischen Client (PC des Nutzers) und der Server (Website des Diensteanbieters) dient, indem es die Website durch digitale Zertifikate authentifiziert und die Kommunikation verschlüsselt abwickelt.
[844] Telekommunikations-Datenschutzrichtlinie (Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15.12.1997, ABl. EG Nr. L 24 vom 30.01.1998, S. 1, über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation) ist von der EU-Richtlinie 2002/58/EG abgelöst worden (vgl. hierzu Eckhardt, CR 2003, 805, 805).

anzubieten, ist daher nicht folgerichtig. Verschlüsselungen stellen Maßnahmen dar, die allein von Anbieter von Telediensten erfüllt werden können.[845]

Aber auch wenn dem Access-Provider, anders als dem Betreiber eines lokalen Netzwerkes, wie beispielsweise eines W-Lan,[846] nicht möglich ist, die Verschlüsselung zu selbst bewerkstelligen, so kann er immerhin durch sein Expertenwissen entsprechende Aufklärung und Information über die verschiedenen Verschlüsselungstechniken gemäß § 109 Abs. 1 TKG leisten. Dies stellt insoweit eine Maßnahme dar, die einen Provider nicht über Gebühr belastet, sofern er über gängige Verschlüsselungstechniken wie beispielsweise Secure Socket Layer (SSL) informiert.[847]
Ein Access-Provider mit eigenem Backbone[848] kann darüber hinaus innerhalb seines Backbones die MPLS-Technik einsetzen, mit der bewerkstelligt werden kann, dass Angriffe auf Daten zumindest erschwert werden.[849]

---

[845] Vgl. zu dieser Auffassung Koenig/Röder, CR 2000, 668, 671.
[846] Vgl. Zimmer, CR 2003, 893, 897 und Dornseif/Schumann/Klein, DuD 2002, 226 ff. Zum W-Lan siehe außerdem S. 139.. Zimmer, CR 2003, 893, 897 legt es in die Verantwortung des W-Lan-Betreibers für eine entsprechende Verschlüsselung des W-Lan-Netzes zu sorgen. Zu berücksichtigen ist aber, dass dies lediglich bei drahtlosen Büronetzwerken eine solche Verantwortung des Betreibers normiert werden kann, da der Betreiber in diesem Falle auch die Ausstattung der einzelnen Rechner mit der entsprechenden Client-Software vornehmen kann. Aber bei Hotels, Flughäfen, Cafes, auf die Zimmer (Zimmer, CR 2003, 893, 896) Bezug nimmt, ist eine Verschlüsselung nur dann möglich, sofern auch die einzelnen Rechner entsprechend ausgerüstet sind. Dornseif/Schumann/Klein, DuD 2002, 226 ff. stellen dar, dass die Basisstationen von W-Lans grundsätzlich Authentifizierungsfunktion (Dornseif/Schumann/Klein, DuD 2002, 226, 227) und Verschlüsselungsfunktion (Dornseif/Schumann/Klein, DuD 2002, 226, 228) übernehmen können. Für eine Authentifizierung müssen aber die einzelnen Rechner ein Passwort besitzen, so dass bei einer „open system Konfiguration“ praktisch keine Authentifizierung in Betracht kommt (vgl. Dornseif/Schumann/Klein, DuD 2002, 226, 227). Auch bei einer Verschlüsselung ist generell notwendig, dass gleichermaßen die einzelnen Rechner entsprechende Verschlüsselungsprogramme enthalten (siehe zur Verschlüsselung auch S. 41 ff. in dieser Arbeit), so dass ebenso in der Verantwortung des einzelnen Nutzers liegt, für den Schutz seiner Nachrichten Sorge zu tragen und Verschlüsselung einzusetzen. Damit liegt die Netzsicherheit bei offenen W-Lans, wie Flughäfen; Hotels, etc. nicht nur in der alleinigen Verantwortung des W-Lan-Betreibers. Der W-Lan-Betreiber kann allerdings die Basisstationen so einrichten, dass diese ohne Aktivierung von Verschlüsselung von vorneherein keine Nutzung zulassen.
[847] Zu SSL siehe oben S. 196 ff. Siehe hierzu auch die Ausführungen von Koenig/Röder, CR 2000, 668 ff. bezüglich der EG-Datenschutzrichtlinie, welche wie oben dargestellt (S. 8 Fn. 29), von der EU-Richtlinie 2002/58/EG abgelöst worden ist. Die Verfasser gehen davon aus (aaO 671/672), dass im Sinne der Richtlinie jeder Diensteanbieter geeignete technische und organisatorische Maßnahmen, wie etwa Verschlüsselung, ergreifen muss, um die Sicherheit seiner Dienste zu gewährleisten, insoweit die Netzsicherheit davon betroffen ist.
[848] Siehe zum Begriff des Backbones S. 28.
[849] Siehe zu MPLS S. 34.

Ob der Access-Provider mit eigenem Backbone[850] zum Einsatz von MPLS verpflichtet ist, hängt unter anderem vom finanziellen Aufwand dieser Technik ab.[851] Es muss dementsprechend an technische Experten die Frage gestellt werden, ob MPLS mittlerweile Stand der Technik ist und ob MPLS dazu beiträgt, ein notwendiges Schutzniveau zu erreichen bzw. ob dieses Schutzniveau ebenso gut durch andere technische Maßnahmen erreicht werden kann.[852]
Insbesondere müssen hier die Kosten für die Provider berücksichtigt werden, und ob es wirtschaftlich vertretbar ist, sämtliche Netze mit dieser Technik auszustatten.

bbb. Anforderungen an den Internetzugangsknoten

Den Internetzugangsknoten als Telekommunikationsanlage[853] muss der Provider so einrichten, dass den Sicherheitserfordernissen des § 109 Abs. 2 TKG genüge getan ist, da er eine Telekommunikationsdienstleistung für die Öffentlichkeit gemäß § 3 Nr. 19 TKG a.F. erbringt.[854]
Ein Internetzugangs-Provider erbringt eine Telekommunikationsdienstleistung für die Öffentlichkeit, da er für eine Vielzahl von Kunden und einer Allgemeinheit den Internetzugang bereitstellt, die nicht voneinander abgrenzbar sind.[855] Für das Tatbestandsmerkmal der Öffentlichkeit ist im Übrigen ausreichend, dass ein bereits im Einzelnen definiertes Angebot vorliegt, aus dem sich jeder Kunde sein individuelles Leistungspaket zusammenstellen kann.[856]

---

[850] Vgl. auch Summa in: Holznagel/Nelles/Sokol, TKÜV, S. 25, der anmerkt, dass die beiden größten Internet-Anbieter T-Online und AOL über keine eigene Infrastruktur verfügen, sondern sich diese von einem oder mehreren Providern mit Backbone zur Verfügung stellen lassen. Er bezeichnet diese Provider ohne eigene Infrastruktur als „virtuelle Provider".
[851] Siehe zu den Kriterien eines „mittleren Schutzniveaus" Zimmer, CR 2003, 893, 897, die außerdem das Expertenwissen und das Entdeckungsrisiko bei Angriffen benennt.
[852] Siehe zum Vergleich zwischen IPSec und MPLS auch die Informationen unter http://www.claranet.de./ipservices/vpn/. Ein Vergleich zwischen IPSec und MPLS findet sich ebenso bei Böhmer, Virtual Private Networks (2. Auflage), S. 379 ff. Auf S. 380 wird darauf hingewiesen, dass IPSec auch in Verbindung mit MPLS eingesetzt werden kann.
[853] Siehe hierzu Büchner in: TKG-Kommentar, § 85 TKG Rn. 2; Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 11; Haß in: Manssen, Manssen, Kommentar Telekommunikations- und Multimediarecht, § 85 TKG(1998), Band 1, Rn. 11.
[854] Siehe zum Telekommunikationsdienst für die Öffentlichkeit S. 116.
[855] Vgl. zur geschlossenen Benutzergruppe insbesondere die Ausführungen auf S. 184 ff.
[856] Vgl. Schütz in: TKG-Kommentar (2. Auflage), § 3 TKG Rn. 22a.

So obliegt nach § 109 Abs. 2 TKG den Betreibern von Telekommunikationsanlagen darüber hinaus die technische Verpflichtung den betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und von Telekommunikations- und Datenverarbeitungssystemen gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen.[857] Der Umfang der Schutzmaßnahmen ist gesetzlich nicht festgelegt.[858] Es besteht lediglich ein unverbindlicher Katalog von Sicherheitsanforderungen.[859] Als notwendig wird jedoch ein dem Stand der Technik angepasstes, „mittleres Schutzniveau" erachtet, welches den Zugriff hinreichend erschwert, wobei Expertenwissen und finanzieller Aufwand ebenso mit einzubeziehen sind.[860]

Im Hinblick auf die Authentifizierung am Internetzugangsknoten bzw. RADIUS-Server gilt, dass der Provider verpflichtet ist, den Grundsatz des Systemdatenschutzes gemäß § 3a BDSG zu beachten, und solche Authentifizierungssysteme einzusetzen, die eine pseudonyme Nutzung ermöglichen. Eine Authentifizierung mittels Namen der Nutzer ist daher zu vermeiden, soweit es andere gleichwertige Authentifizierungsmöglichkeiten gibt.[861]
Eine solche Verpflichtung gehört aber nicht nur zu den Maßnahmen einer adäquaten Datenvermeidung, sondern stellt darüber hinaus eine Maßnahme dar, die der Provider als Diensteanbieter gemäß § 3 Nr. 6 TKG im Sinne von §§ 88, 109 Abs. 1 TKG zu treffen hat. Es sind technische und organisatorische Schutzvorkehrungen zur Verhinderung unbefugter Kenntnisnahme von

---

[857] Siehe hierzu auch Röhrborn/Katko, CR 2002, 882, 887; Gola/Klug, Grundzüge des Datenschutzrechts, S. 199.

[858] Zur Einholung einer Verpflichtungserklärung, die die Verpflichtung der Mitarbeiter auf das Datenschutzgeheimnis nach § 5 BDSG beinhaltet, siehe auch Königshofen, RDV 1997, 97, 99.

[859] 1997 ist vom damaligen Bundesministerium für Post und Telekommunikation zu § 87 TKG a.F ein Katalog von Sicherheitsanforderungen erstellt worden, siehe hierzu Zimmer, CR 2003, 893, 896 und Groß in: Roßnagel, Handbuch Datenschutzrecht, 7.8 Rn. 21. Siehe außerdem IT-Grundschutz-Kataloge, Sicherheit in der Informationstechnik, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik, Loseblattsammlung, Stand2005, abrufbar unter www.bsi.de.

[860] Zimmer, CR 2003, 893, 896 ff.; Zerres in: Scheurle/Mayen, TKG-Kommentar, § 87 TKG Rn. 17 ff.; Trute in: Trute/Spoerr/Bosch, TKG-Kommentar, § 87 TKG Rn. 14.

[861] Zu den Möglichkeiten der Authentifizierung siehe etwa Lipp, VPN, Lipp, VPN, S. 56, 145 ff.

erhobenen und gespeicherten Verbindungsdaten zu erfüllen.[862] Da ebenso Benutzerkennungen gemäß § 96 Abs. 1 Nr. 1 TKG Verbindungsdaten darstellen können, bedeutet dies, dass der Provider gleichfalls darauf zu achten hat, dass er die Benutzerdaten vor unbefugter Kenntnisnahme schützt.

Diese Überlegungen sind auch aus dem Grunde von Bedeutung, da die Bundesnetzagentur bei Nichterfüllung von datenschutzrechtlichen Verpflichtungen den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise gemäß § 115 Abs. 3 TKG untersagen kann. Die Bundesnetzagentur ist darüber hinaus gemäß § 115 Abs. 2 Nr. 2 TKG befugt, ein Zwangsgeld bis bis zu 100.000 Euro zur Durchsetzung der Verpflichtungen nach den § 109 TKG zu erheben.

cc. Auskunfts- und Überwachungsmaßnahmen

Anbieter von geschäftsmäßig erbrachten Telekommunikationsdiensten sind gemäß § 113 TKG zur Auskunft über verarbeitete Daten und/oder im Sinne der TKÜV zur Überwachung verpflichtet.[863].
Gemäß § 1 TKÜV ist erforderlich, dass ein Telekommunikationsdienst für die Öffentlichkeit erbracht wird (§ 3 Nr. 19 TKG a.F.).[864] Dies ist bei einem Internetzugangsknoten, wie gerade festgestellt, zwar der Fall, aber nach § 3 Abs. 2 Nr. 2 TKÜV ist der Betreiber eines Internetzugangsknotens von der Verpflichtung befreit, Maßnahmen vorzuhalten.[865]
Dies hat jedoch keinen unmittelbaren Einfluss auf das Verhältnis zwischen Provider und VPN-Auftraggeber, da der Internetzugangs-Provider gemäß § 113 Abs. 1 S. 3 TKG dennoch auf Anordnung der berechtigten Stelle im Sinne von § 2 Nr. 3 TKÜV, § 1 Abs. 1 Nr. 1 des G-10-Gesetzes, § 100b Abs. 3 Satz 1 StPO, § 23a Abs. 1 S. 1 des Zollfahndungsdienstegesetzes oder nach Landesrecht

[862] Vgl. Post-Ortmann, RDV 1999, 102, 103.
[863] Zur TKÜV siehe S. 12, insbesondere Fn. 46.
[864] Zum Telekommunikationsdienst für die Öffentlichkeit Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 100 sowie siehe S. 116 in dieser Arbeit.
[865] Siehe Holznagel/Enaux/Nienhaus, Telekommunikationsrecht, Rahmenbedingungen – Regulierungspraxis, Rn. 708.

verpflichtet ist, Überwachungsmaßnahmen zu ermöglichen.[866] Lediglich im Verhältnis zwischen Provider und Behörde hat die Frage, ob Maßnahmen zur Überwachung vorgehalten werden müssen, wegen der entsprechenden Kostentragungspflicht Relevanz.

Der VPN-Auftraggeber sollte also (ebenso wie jeder andere Kunde, der einen Internetzugang beauftragt) bedenken, dass der Provider, der den Access bereit stellt, Überwachungsmaßnahmen und Auskunftsverpflichtungen zu erfüllen hat.

Zu beachten ist hierbei allerdings die Wahrnehmung der unterschiedlichen Funktionen seitens des Providers innerhalb eines „Komplettpaket VPN"[867] sowie die unterschiedlichen technischen Systeme „Internetzugangsknoten" und „Gateway". Ob und welche Überwachungsmaßnahmen den Provider treffen, sofern er außerdem das Management des Gateway übernimmt wird an späterer Stelle dargestellt.[868]

b. Notwendige Infrastruktur

Da es das Ziel dieser Arbeit ist, die datenschutzrechtlichen Pflichten sämtlicher an einem VPN beteiligten Personen feststellen und voneinander abgrenzen zu können, sind in die Betrachtung ebenso die Anbieter der Infrastruktur des Internet mit einzubeziehen (TK-Provider, DNS-Server-Betreiber sowie Routerbetreiber).[869]
Auch diesen obliegen die im zweiten Abschnitt dargestellten Pflichten bezüglich Datenschutz und Datensicherheit, zu denen die Datenvermeidung und die technischen Schutzmaßnahmen zählen.[870] Darüber hinaus soll Berücksichtigung finden, dass der Datenschutz durch gesetzliche Überwachungsmaßnahmen oder Auskunftsverpflichtungen eingeschränkt sein kann.[871]

[866] Vgl. Holznagel/Enaux/Nienhaus, Telekommunikationsrecht, Rahmenbedingungen – Regulierungspraxis, Rn. 708.
[867] Siehe zu dem Begriff „Komplettpaket VPN" die Ausführungen auf S. 4.
[868] Siehe hierzu die Ausführungen auf S. 230 ff.
[869] Siehe zur notwendigen Infrastruktur S. 140.
[870] Siehe S. 106 ff. sowie S. 162.
[871] Siehe den Verweis in der vorherigen Fußnote.

Daher wird im Folgenden untersucht, inwieweit dem TK-Provider, dem DNS-Server-Betreiber sowie dem Routerbetreiber als Anbieter der notwendigen Infrastruktur datenschutzrechtliche Pflichten obliegen.

aa. Datenvermeidung

aaa. TK-Providing

Zur notwendigen Infrastruktur des Access-Providing gehört das TK-Providing.[872] Somit orientiert sich die nachfolgende datenschutzrechtliche Prüfung an den für das Access-Providing relevanten Daten.

(1) Anschlussnummer und Zielrufnummer

Der TK-Provider erhält Kenntnis über die Anschlussnummer.[873]
Gemäß § 96 Abs. 1 Nr. 1 TKG stellt dieses Datum (Nummer des beteiligten Anschlusses) ein Verkehrsdatum dar.[874]
Da die Anschlussnummer für den Aufbau weiterer Verbindungen notwendig ist, darf und muss der TK-Provider diese über den Verbindungsvorgang hinaus speichern. Werden dem TK-Provider weitere Daten, wie Datum, Uhrzeit, Dauer der Verbindung oder IP-Adresse bekannt,[875] sind diese unverzüglich zu löschen. Etwas anderes gilt, soweit der TK-Provider diese für seine Zwecke im Sinne von §§ 97, 99 und 100 TKG benötigt. Daher kann eine längerfristige Speicherung (deren Dauer jedoch im Einzelfall zu bestimmen ist) in Betracht kommen. Es empfiehlt sich auch hier, in die wirtschaftliche Betätigungsfreiheit von Unternehmen nicht insoweit einzugreifen, dass feste Löschungsfristen vorgegeben werden.[876] Insgesamt gilt auch beim TK-Providing, dass mehr Datenschutz „gewonnen" wird, sofern ein Unternehmen im Sinne eines

[872] Vgl. oben S. 141.
[873] Vgl. Köhntopp/Köhntopp, CR 2000, 248, 250; Schaar, Datenschutz im Internet, Rn. 171.
[874] Siehe zur datenschutzrechtlichen Relevanz der Anschlussnummer auch Gola/Schomerus, BDSG, § 3 BDSG Rn. 6.
[875] Schaar, Datenschutz im Internet, Rn. 171, verweist darauf, dass im Falle der Herstellung einer Internetverbindung über ein öffentliches Telekommunikationsnetz von der Telefongesellschaft für Zwecke der Telefonabrechnung die Nummer des Anrufers mit Datum, Stunde und Dauer aufgezeichnet wird.
[876] Insoweit wird auf die obigen, zum Access-Providing gemachten Ausführungen verwiesen (Siehe S. 170 ff.).

wirksamen und verantwortungsbewussten Datenschutzes die gesetzlichen Höchstspannen der §§ 97 Abs. 3, 100 Abs. 3 TKG für die Datenspeicherung nutzt, als wenn gesetzliche Mindestspeicherungsfristen eingeführt werden, die letztendlich zu einer staatlich vorgegebenen Vorratsdatenspeicherung führen.[877]

Als weiteres datenschutzrechtlich relevantes Datum kann hier die Zielrufnummer des Internetzugangsknotens (PoP, Einwahlserver) in Betracht kommen, sofern der TK-Provider die Einwahlgebühren separat berechnet. Sofern der Kunde dies gemäß § 97 Abs. 4 Nr. 1 TKG verlangt, muss der TK-Provider diese Nummer um die letzten drei Ziffern zu kürzen.
Erfolgt keine separate Berechnung der Einwahlkosten,[878] sondern bietet der Access-Provider beispielsweise einen Pauschaltarif an oder nimmt der Access-Provider eine eigenständige Rechnungsstellung vor,[879] dann benötigt der TK-Provider die Zielrufnummer (des PoP) von vorneherein nicht, so dass ihre Speicherung, auch unter Berücksichtigung einer Datenvermeidung, nicht erforderlich ist.[880]

(2) Standortdaten

Für den TK-Provider gilt entsprechend der obigen Ausführungen zum Access-Providing, dass er ohne Anonymisierung oder Einwilligung des VPN-Auftraggebers bzw. Teilnehmers „einfache“[881] Standortdaten verarbeiten darf, aber im Sinne von § 96 Abs. 2 TKG nur für die Dauer der Verbindung. Dies ergibt sich auch aus § 96 Abs. 1 Nr. 1 TKG.[882]

---

[877] Siehe insbesondere S. 179. Siehe außerdem zur grundsätzlich restriktiven Auslegung des Rechts auf Protokollierung, Bizer, DuD 2006, 270, 273.
[878] Siehe oben S. 189 ff. und Kroiß/Schuhbeck, Jura online, S. 5/6.
[879] Eine eigenständige Rechnungsstellung dürfte sehr selten der Fall sein, da regelmäßig sämtliche Provider ihre Rechnungsstellung über die Deutsche Telekom AG vornehmen. Siehe auch Frankfurter Allgemeine Zeitung vom 18.Juni 2004, S.12 mit der Meldung, dass künftig ein erweitertes Dienstespektrum bei der Abrechnung der von Wettbewerbern angebotenen Mehrwertdiensten durch die Telekom gelten soll. Dies wurde zwischen der Telekom und dem Verband der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM) vereinbart. So ist im Rahmen einer Branchenlösung des VATM geplant, eine zentrale Datenbank mit den Verbindungsdaten aufzubauen, um die Dienste unabhängig vom Netzbetreiber abrechnen zu können.
[880] Siehe hierzu insbesondere auch S. 106 ff.
[881] Damit sind Standortdaten gemeint, die nicht für einen Dienst mit Zusatznutzen verarbeitet werden sollen.
[882] Siehe S. 190 ff.

Sofern der TK-Provider einen Dienst mit Zusatznutzen erbringt, oder die Daten an den Access-Provider weitergibt, damit dieser etwa eine Beratung hinsichtlich der günstigsten Tarife am jeweiligen Standort durchführen kann,[883] so bedarf er für diese Weitergabe ebenso einer Einwilligung des Teilnehmers. Dies ergibt sich aus § 96 Abs. 2 TKG, wonach Verkehrsdaten unverzüglich nach Ende der Verbindung, hier also durch den Netzbetreiber, zu löschen sind.[884]
Der TK-Provider ist in diesem Zusammenhang entsprechend den Verpflichtungen des Access-Providers gemäß § 93 TKG außerdem verpflichtet, über die grundlegenden Verarbeitungstatbestände zu unterrichten.[885]
Hier kann allerdings die Schwierigkeit hinzukommen, dass ein Mobilfunknetzbetreiber in unterschiedlichen geografischen Bereichen eine unterschiedliche Anzahl von Basisstationen oder Funkzellen haben kann, so dass sich die Ortungsmöglichkeiten unter Umständen in den verschiedenen geografischen Bereichen ändern.
Nichtsdestotrotz wäre für einen Mobilfunkbetreiber eine Unterrichtung aber in der Form leicht zu erfüllen, dass er *beispielsweise in der Regel über ein Netz von 100 Basisstationen in einem Umkreis von 200 km verfügt, und im Stadtgebiet von X-Stadt sogar über 250*. Der Mobilfunkbetreiber muss zumindest im Bereich des für ihn praktisch Machbaren zur Unterrichtung gemäß § 93 TKG verpflichtet sein.

In rechtspolitischer Hinsicht ist interessant, dass nach § 98 TKG letztendlich der Telekommunikationsdiensteanbieter, also ebenso der TK-Provider bzw. der Netzbetreiber die Verantwortung dafür trägt, dass Standortdaten im Zusammenhang mit Diensten von Zusatznutzen nur in dem dafür erforderlichen Zeitraum verwendet werden. So muss der TK-Provider nach § 98 Abs. 2 TKG

[883] Siehe hierzu Erwägungsgrund 18 der EU-Richtlinie 2002/58/EG.
[884] Siehe in diesem Zusammenhang auch die obigen Ausführungen zum Access-Provider S. 190 ff. Klarstellend ist anzumerken, dass der Access-Provider verpflichtet ist, sofern er Standortdaten auch nach Ende der Verbindung oder zur Bereitstellung von Diensten mit Zusatznutzen benötigt, gemäß § 96 Abs. 3 TKG die Einwilligung des Teilnehmers einzuholen und ihn nach § 96 Abs. 4 TKG umfassend über die Dauer der Speicherung sowie sein jederzeitiges Widerrufsrecht zu informieren. Im Übrigen ist zu beachten, dass der Access-Provider beim (zusätzlichen) Angebot eines Dienstes mit Zusatznutzen selbst dann eine Einwilligung zur Verwendung von Standortdaten einholen muss, sofern er diese Daten (auch) für Zwecke der Entgeltabrechnung nach § 97 Abs. 5 TKG benötigt. Denn hier handelt es sich um die Weitergabe von Standortdaten.
[885] Siehe S. 110 ff. Im Hinblick auf die Informations- und Löschungspflichten siehe auch die Ausführungen zum Access-Provider, insbesondere auf S. 196 ff.

dafür Sorge tragen, dass die Teilnehmer die Verarbeitung der Standortdaten jederzeit untersagen können.

Sofern die weitere Datenverarbeitung von einem Telekommunikationsdiensteanbieter bzw. einem Access-Provider vorgenommen wird, ist diese Fragestellung im Hinblick auf die Sicherstellung eines „ausreichenden Datenschutzniveaus“ ohne größere praktische Relevanz. In diesem Fall schützt § 96 Abs. 3 TKG den Teilnehmer vor übereilten und den Schutz seiner Daten betreffenden Entscheidungen, da er hier nochmals einwilligen muss.
Ein Telekommunikationsdiensteanbieter bzw. ein Access-Provider muss gemäß § 96 Abs. 3 TKG vor einer Standortdatenverarbeitung ebenso die Einwilligung der Teilnehmer einholen, sofern er einen Dienst mit Zusatznutzen anbietet. Das Angebot eines Dienstes mit Zusatznutzen kann bei einem Access-Provider etwa in Betracht kommen, wenn er seinen Teilnehmern standortabhängig eine Beratung über die Tarife anbietet.[886]

Schwierigkeiten bezüglich der Sicherstellung eines „ausreichenden Datenschutzniveaus“ ergeben sich jedoch dann, sofern die weitere Datenverarbeitung durch einen Telediensteanbieter gemäß § 2 Abs. 1 TDG vorgenommen wird. Denn diesbezüglich gelten aufgrund des TDDSG eigene datenschutzrechtliche Erfordernisse.
Ein Anbieter von standortabhängigen touristischen Informationen, der nicht (gleichzeitig) Access-Provider ist und damit keinen Telekommunikationsdienst erbringt, ist gerade nicht gemäß § 96 Abs. 3 TKG daran gebunden, eine separate Einwilligung des Teilnehmers für die Dauer des Dienstes mit Zusatznutzen einzuholen, und im TDDSG ist kein separates Einwilligungserfordernis bezüglich Standortdaten zu finden. Dennoch erbringt der Anbieter gemäß § 2 Abs. 1 TDG durch den Dienst mit Zusatznutzen, z.B. der touristischen Informationen, zumindest auch einen Teledienst.[887]
Dies kann dann problematisch sein, wenn der Internetzugang nicht als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG, sondern als Teledienst

[886] Siehe Erwägungsgrund 18 der EU-Richtlinie 2002/58/EG.
[887] Vgl. hierzu S. 102 ff.

eingeordnet wird.[888] In diesem Falle kommen die datenschutzrechtlichen Regelungen der TDDSG zur Anwendung und der Access-Provider, an welchen der TK-Provider die Daten weitergegeben hat, muss zwar über Art, Umfang und Zweck seiner Nutzung gemäß § 4 Abs. 1 TDDSG aufklären.[889] Diese Regelung ist vergleichbar mit der Intention der EU-Richtlinie 2002/58/EG sowie den Informationspflichten des Access-Providers nach § 96 Abs. 3, Abs. 4 TKG, da unter § 4 TDDSG insbesondere auch die vorgesehene Dauer der Speicherung fällt.[890]

Unterschiede gibt es jedoch bei den Nutzungsdaten.[891] Der Telediensteanbieter darf Nutzungsdaten gemäß § 6 Abs. 1 TDDSG ohne weitere Einwilligung des Nutzers für den Dienst mit Zusatznutzen verarbeiten, sofern dies für die Inanspruchnahme des Dienstes erforderlich ist.

Dies bedeutet, dass ein Telediensteanbieter anders als ein Anbieter eines Telekommunikationsdienstes gemäß § 96 Abs. 3 TKG anfallende Standortdaten ohne Einwilligung des Nutzers verarbeiten darf und nicht anonymisieren muss.

Schutz besteht zwar dahingehend, dass sich aus dem Umkehrschluss von § 96 Abs. 2 TKG ergibt, dass die Standortdaten nur unter Einwilligung des jeweiligen Nutzers an einen Telediensteanbieter weitergegeben werden dürfen. Abweichungen ergeben sich jedoch im Rahmen der Verarbeitung, da nach derzeitiger Gesetzesfassung allenfalls der Telekommunikationsdiensteanbieter dafür Sorge tragen müsste, dass die Standortdaten nur in der Zeit verarbeitet werden, für die der Teledienst angeboten wird. Eine Verpflichtung des Dritten (Telediensteanbieters) besteht jedoch nicht. Kritisch ist allerdings anzumerken, dass eine gesetzliche Klarstellung fehlt, ob Access-Providing als Telekommunikationsdienst oder Teledienst einzuordnen ist. [892] Vor diesem Hintergrund hätte zumindest im TDDSG eine Regelung Berücksichtigung finden sollen, nach der gleichermaßen Telediensteanbieter, soweit sie Standortdaten

---

[888] Siehe hierzu die Ausführungen auf S. 122 ff.

[889] Zu den Unterrichtungspflichten des § 4 Abs. 1 TDDSG a.F. siehe unter anderem Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 94/95 mit dem Hinweis, dass die in der alten Fassung des § 4 Abs. 1 TDDSG festgelegte Unterrichtungspflicht „vor der Erhebung“ im Hinblick auf IP-Adressen einem Diensteanbieter und Betreiber eines Web Servers, der die IP-Adressen der Nutzer bei jedem Zugriff auf die aufgerufene Website speichert, unmöglich gewesen ist.

[890] Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 127.

[891] Siehe zu diesem Begriff S. 104 ff.

[892] Siehe hierzu die Ausführungen auf S. 122 ff.

für ihre Dienste verarbeiten bzw. um damit standortbezogene Dienste zu leisten, diese Standortdaten nur für den Zeitraum der Diensterbringung und mit Einwilligung des Nutzers verarbeiten dürfen.

Dies gilt ebenso für andere Telediensteanbieter, die die Erstellung eines detaillierten Bewegungsprofils für ihre Dienste benötigen.[893]
Eine Regelung wie folgt hätte daher für Klarheit gesorgt: *Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten verwendet werden* ***und die für die Erstellung eines Bewegungsprofils geeignet sind, um ein solches Bewegungsprofil für Angebote im Sinne von § 2 TDG zu nutzen,*** *dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat.*

bbb. DNS-Betreiber

Da der DNS-Server-Betreiber einen Teil der notwendigen Infrastruktur des Access-Providing bereitstellt, sind auch dessen datenschutzrechtliche Pflichten zu prüfen und von den Pflichten anderer Anbieter abzugrenzen.[894]

(1) DNS-Service

Es wurde bereits festgestellt, dass DNS-Server-Betreiber an der Erbringung eines Telekommunikationsdienstes mitwirken, da sie eine Zuordnung zwischen IP-Adresse zu einem Domain-Namen vornehmen.[895] Dieser Umstand gilt sowohl für jeden Websitebetreiber im Internet als auch in einem VPN, sofern der „angerufene" Standort nicht nur über eine feste IP-Adresse, sondern ebenso über einen Domain-Namen verfügt.

[893] Vgl. hierzu auch Schrey/Meister, K&R 2002, 177, 179.
[894] Siehe zur notwendigen Infrastruktur S. 140.
[895] Siehe S. 141 ff.

Zur Legitimation der (erstmaligen) Speicherung der Zuordnung von fester IP-Adresse zu Domain-Namen auf einem DNS-Server sind im TKG keine spezifischen Regelungen vorgesehen.[896]
So geht § 3 Nr. 30 TKG lediglich davon aus, dass Verkehrsdaten „bei der Erbringung von Telekommunikationsdiensten“ anfallen, aber der Vorgang der Verknüpfung bzw. Zuordnung zwischen fester IP-Adresse und Domain findet zeitlich betrachtet bereits zuvor statt und nicht erst „bei“ der Erbringung eines Telekommunikationsdienstes. Der Telekommunikationsdienst „Access-Providing“ kann vielmehr erst stattfinden, wenn die Zuordnung bereits vorliegt. Die Legitimation zur Speicherung der Zuordnung von fester IP-Adresse zu Domain-Namen ergibt sich aber für den DNS-Server-Betreiber aus § 28 Abs. 1 Nr. 1 BDSG. Aus der Anwendbarkeit des BDSG folgt, dass im Hinblick auf VPN-Auftraggeber, die als juristische Personen oder Personengesellschaften einzuordnen sind, die Speicherung der Zuordnung zwischen IP-Adresse und ihrem Domain-Namen auf einem DNS-Server ohne weiteres zulässig ist.

Lediglich bei der Beauftragung eines VPN durch natürliche Personen sind die Voraussetzungen des § 28 Abs. 1 Nr. 1 BDSG separat zu prüfen und aus den folgenden Gründen zu bejahen:[897]
In § 28 Abs. 1 Nr. 1 BDSG ist geregelt, dass das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist (und zwar ohne weitere Einwilligung), wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichem Vertrauensverhältnisses mit dem Betroffenen dient. Dienen ist hierbei im Sinne eines „Müssen“ zu verstehen.[898]
Zwischen DNS-Server-Betreiber und Kunde bzw. VPN-Auftraggeber (der als natürliche Person einzuordnen ist) kommt ein vertragsähnliches

[896] Vgl. etwa Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 101 zum Exklusivitätsverhältnis von BDSG und TDDSG sowie §§ 91 ff. TKG. Siehe außerdem die Ausführungen auf S. 92 in dieser Arbeit. Wenn von vorneherein keine Priorität der datenschutzrechtlichen Regelungen von TDDSG oder §§ 91 ff. TKG besteht, und sich die Regelungsbereiche nicht überschneiden, so spricht nichts gegen die Anwendbarkeit des § 28 BDSG. § 3 Nr. 3 TKG kommt hier im Übrigen nicht in Betracht, da der DNS-Server-Betreiber, da der DNS-Server-Betreiber keine Teilnehmer gemäß § 3 Nr. 20 TKG hat, mit denen er ein Vertragsverhältnis begründet hat.
[897] Bei Personengesellschaften oder juristischen Personen, die ein VPN beauftragen, ist demgemäß die Speicherung und Verknüpfung ohne weiteres zulässig, da hier das BDSG keine Anwendung findet und das TKG, wie oben dargestellt, nicht einschlägig ist.
[898] Siehe Gola/Schomerus, BDSG, § 28 BDSG Rn. 13, mit dem Hinweis, dass ein „verarbeiten müssen“ zu fordern ist, auch wenn der Gesetzeswortlaut lediglich ein „dienen“ erfasst.

Vertrauensverhältnis in Betracht.[899] Dies ergibt sich anhand der Funktion, welche die DNS-Server-Betreiber wahrnehmen, insbesondere aufgrund der Tatsache, dass der Internetnutzer in seiner Kommunikation von DNS-Server-Betreibern abhängig ist und der DNS-Server zur notwendigen Infrastruktur gehört.[900] Daher lässt sich hier ein solches vertragsähnliches Vertrauensverhältnis bejahen,[901] auch wenn dieses Merkmal grundsätzlich restriktiv zu verstehen ist.[902]
Ein unmittelbares Vertragsverhältnis liegt im Übrigen auch dann nicht vor, wenn der DNS-Server-Provider zugleich die Funktion eines Access-Providers innehat,[903] da im Sinne der in dieser Arbeit entwickelten dienstorientierten[904] Betrachtungsweise auf den jeweiligen Dienst abzustellen ist, und dementsprechend nur im Verhältnis des Kunden bzw. VPN-Auftraggebers zum Access-Provider ein Vertragsverhältnis vorliegt.

Des Weiteren stellt ein DNS-Server-Betreiber die Internet-Kommunikation und Betreuung der Internetnutzer sicher, so dass die Datenverarbeitung des DNS-Server-Betreibers zu eigenen Geschäftszwecken erfolgt,[905] und zwar als Hilfsmittel[906] zur Erfüllung, Abwicklung und Sicherstellung des Internetzugangs und Internet-Kommunikation. Die Speicherung der Zuordnung von fester IP-Adresse zu Domain-Namen gemäß § 3 Abs. 4 Nr. 1 BDSG[907] auf dem DNS-Server ist insoweit nicht Selbstzweck, sondern muss zur Erfüllung anderer Zwecke erfolgen.

---

[899] Siehe zum vertragsähnlichen Vertrauensverhältnis die Ausführungen bei Gola/Schomerus, BDSG, § 28 BDSG Rn. 26 ff.
[900] Siehe S. 140.
[901] Siehe die Ausführungen von Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 66 zu „Anstands- und Treuepflichten" einer engeren vertrauensvollen Beziehung, die einem Vertrag nahe kommt.
[902] Vgl. Simitis in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 120 ff.
[903] Siehe hierzu Anmerkung Spindler zu OLG Hamburg, MMR 2000, 278, 279.
[904] Siehe zur dienstorientierten Betrachtungsweise S. 74/86.
[905] Gola/Schomerus, BDSG, § 28 BDSG Rn. 4; Simitis in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 22; siehe außerdem Hoeren in: Roßnagel, Handbuch Datenschutzrecht, 4.6 Rn. 17 zum Erfordernis des unmittelbaren sachlichen Zusammenhangs zwischen der Speicherung und der Abwicklung des Vertrages.
[906] Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 3. Die Datenverarbeitung gemäß § 28 Abs. 1 Nr. 1 BDSG soll als Mittel zum Zweck, d.h. zur Erreichung eines dahinter stehenden Geschäftszwecks, eines wirtschaftlichen Erfolgs, dienen (siehe Gola/Schomerus, BDSG, § 28 BDSG Rn. 4). Siehe ebenso Simitis in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 22.
[907] Gemäß § 3 Abs. 4 Nr. 1 BDSG bedeutet Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung. Vom Sinn her ist unter Datenträger jedes Medium zu verstehen, das zum Aufnehmen personenbezogener Daten geeignet ist, d.h. auf dem Informationen für eine spätere Wahrnehmung festgehalten werden können (Gola/Schomerus, BDSG, § 3 BDSG Rn. 26).

Dementsprechend ist der DNS-Server-Betreiber im Hinblick auf IP-Adressen und Domain-Namen von natürlichen Personen zur Löschung gemäß § 35 Abs. 2 Nr. 1 und Nr. 3 BDSG verpflichtet, sofern diese Daten nicht mehr für den Verbindungsaufbau benötigt werden. Diese Löschungspflicht eines DNS-Server-Betreibers gilt grundsätzlich bei Beendigung eines Internetauftritts (einer natürlichen Person). Speziell in einem VPN wird die Zuordnung zwischen IP-Adresse und Domain-Namen nicht mehr benötigt, wenn der VPN-Auftraggeber einen Standort nicht länger vernetzt.[908] Bei einer solchen Vertragsbeendigung des VPN-Auftragsverhältnisses und damit verbundener Standortkündigung müsste der DNS-Server-Betreiber dementsprechend die feste IP-Adresse des gekündigten Standorts unverzüglich löschen, da sie (mangels Notwendigkeit für den weiteren Verbindungsaufbau) kein vertragsrelevantes Datum mehr darstellt.

Für juristische Personen hingegen, für die das BDSG keine Anwendung findet, müsste eine Löschung der Zuordnung zwischen fester IP-Adresse und Domain-Namen vertraglich geregelt werden. Hierbei besteht die Schwierigkeit, dass es mehrere DNS-Server im Netzverbund gibt, die von unterschiedlichen Anbietern betrieben werden. Selbst derjenige Provider, mit dem der VPN-Auftraggeber bzw. Kunde den Vertrag über die Zurverfügungstellung des Domain-Namens abgeschlossen hat, hat praktisch keine Möglichkeiten, auf die Löschung der Zuordnung zwischen Domain-Name und IP-Adresse bei sämtlichen DNS-Server-Betreibern einzuwirken.

Zu berücksichtigen ist aber, dass die DNS-Server-Betreiber selbst daran interessiert sind, überflüssige Daten auf ihrem Server zu löschen. So gibt es bereits in praktischer Hinsicht keine Notwendigkeit oder einen besonderen Nutzen für DNS-Server-Betreiber, diese Daten längerfristig zu speichern. Durch eine unverzügliche Löschung kann auch dem Umstand Rechnung getragen werden, dass dem DNS-Server-Betreiber regelmäßig nicht bekannt ist, ob es

[908] Nach § 35 Abs. 2 Nr. 3 BDSG hätte er zwar grundsätzlich die Möglichkeit, die IP-Adresse für (andere) eigene Zwecke weiterhin zu speichern (vgl. Gola/Schomerus, BDSG, § 35 BDSG Rn. 13), dennoch ist davon auszugehen, dass sich eine Legitimationsgrundlage für eine weitere Speicherung nach Vertragsbeendigung nur in Ausnahmefällen in Betracht kommen kann. Denn hier kommt - anders als bei Adressdaten - nicht in Betracht, die statische IP-Adresse nach Beendigung der Dienstleistung noch für Werbezwecke benötigt werden könnte. So nehmen Gola/Schomerus (aaO) darauf Bezug, dass sich nach Wegfall des ursprünglichen Speicherungszwecks (z.B. Abwicklung eines Kaufvertrages mit einem Versandhauskunden) eine neue Legitimationsgrundlage für die weitere Speicherung ergeben kann (z.B. Zusendung von Werbematerial), und damit keine Löschungsverpflichtung der Daten besteht.

sich um die IP-Adresse und den Domain-Namen einer natürlichen oder juristischen Person handelt.

Ergänzend sei noch darauf hingewiesen, dass durch die Zuordnung zwischen fester IP-Adresse und Domain-Namen auf einem DNS-Server die IP-Adresse zu einem allgemein zugänglichen Datum gemäß § 28 Abs. 1 Nr. 3 BDSG wird.[909] So wird nunmehr für den einzelnen Nutzer durch Eingabe bestimmter Befehle in der Eingabemaske des Browsers auf einfache Weise nachvollziehbar, welche feste IP-Adresse welchem Domain-Namen zugeordnet ist.[910] Dies gilt zumindest im Rahmen des für sämtliche Internetnutzer frei zugänglichen Internetauftritts eines Anbieters. Bei einem VPN hingegen sind die Domain-Namen der Standorte regelmäßig lediglich einem kleineren Nutzerkreis bekannt, so dass auch die entsprechende feste IP-Adresse kein allgemein zugängliches Datum darstellt.[911]
Berücksichtigt man hier die vertretene Auffassung, dass im Internet kein belangloses Datum existiert,[912] stellt der DNS-Service ein Beispiel dafür dar, wie Datenspuren im Internet ohne Einwirkungs- bzw. Korrekturmöglichkeiten seitens des jeweiligen Teilnehmers grundsätzlich entstehen können.

(2) Dynamischer DNS-Service

Etwas anderes ergibt sich jedoch im Hinblick auf den dynamischen DNS-Service,[913] bei welchem „feste“[914] Domain-Namen einer dynamischen IP-Adresse zugeordnet werden, um einen Verbindungsaufbau zu ermöglichen. Auf dem dynamischen DNS-Server wird der Domain-Name und die jeweils dynamische IP-Adresse gespeichert, so dass dem Access-Provider des die

---

[909] Siehe zu den allgemein zugänglichen Quellen, wie etwa dem Internet, Gola/Schomerus, BDSG, § 28 BDSG Rn. 45. Vgl. außerdem Hoeren in: Roßnagel, Handbuch Datenschutzrecht, 4.6 Rn. 35 mit dem Hinweis, dass die Informationsquelle technisch zur Eignung bestimmt sein muss, der Allgemeinheit, d.h. einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen.
[910] Dies kann der Nutzer durch Eingabe des „ping“-Befehls in der Eingabeaufforderung in einfacher Form nachvollziehen. Siehe außerdem die Möglichkeiten unter www.dnsstuff.com.
[911] Siehe aber die Möglichkeiten unter www.dnsreport.com. Hier kann ein beliebiger Domain-Name eingegeben werden und es werden anschließend die diesem Domain-Namen zugeordneten IP-Adressen aufgelistet, und zwar auch die IP-Adressen, die für Mitarbeiter als Zugang zum internen Firmennetzwerk eingerichtet worden sind.
[912] Vgl. Hornung, MMR 2004, 3, 4.
[913] Siehe hierzu S. 56.
[914] Vgl. das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 236.

Verbindung aufbauenden Standorts bei entsprechender Rückfrage beim dynamischen DNS-Server bekannt ist, zu welchem Standort er die Verbindung aufbauen muss.[915]

Insbesondere handelt es sich bei der dynamischen IP-Adresse um ein Verkehrsdatum gemäß § 3 Nr. 30 TKG, da dies ein Datum darstellt, welches „bei“ der Erbringung eines Telekommunikationsdienstes anfällt. Bei einem dynamischen DNS-Server werden im Rahmen des Telekommunikationsdienstes dynamische IP-Adressen fortwährend neu vergeben. Hier besteht also ein Unterschied zu dem oben dargestellten „DNS-Server“, auf welchem dauerhaft die feste IP-Adresse mit dem Domain-Namen verknüpft werden muss. Der Access-Provider des jeweiligen Internetnutzer, der auf den Server eines Anbieters (mit dynamischer IP-Adresse) zugreifen möchte, muss die jeweils vergebene dynamische IP-Adresse beim Betreiber des dynamischen DNS-Servers erst erfragen, um die Internetverbindung erstellen zu können.[916]

Die Speicherung der Logdaten[917] einer solchen Anfrage durch den Provider auf dem dynamischen DNS-Server sind im Verhältnis zwischen DNS-Server-Betreiber und VPN-Auftraggeber aus datenschutzrechtlicher Sicht unproblematisch. Dies stellt einen Umstand dar, der ausschließlich den Provider betrifft. Es handelt sich um „seine“ Anfrage und der DNS-Server-Betreiber kann nicht nachvollziehen, für welchen Nutzer er nachfragt. Er registriert nur, dass der Provider XY die IP-Adresse für eine Domain erfragt, so dass in diesem weiteren Personenverhältnis zwischen Provider und DNS-Server-Betreiber zu prüfen wäre, ob und inwieweit eine Löschung der Log-Files

[915] Diesbezüglich ist wie folgt zu unterscheiden: Der Access-Provider des Clients vergibt eine dynamische IP-Adresse an den Client, damit dieser eine Verbindung aufbauen kann. Darüber hinaus vergibt der (Access-) Provider des Servers beim dynamischen DNS-Verfahren ebenso eine dynamische IP-Adresse an den Server, damit dieser erreichbar ist. Davon unabhängig ist, dass der Provider des Servers auch zugleich Provider des Client sein kann, wobei er dann jedoch unterschiedliche Funktionen wahrnimmt.
[916] Hierfür ist erforderlich, dass der VPN-Auftraggeber, der Zugriff auf seinen Unternehmensserver gewähren möchte, stets online ist (beispielsweise mittels einer Flatrate). Siehe außerdem die Ausführungen auf S. 30 ff., wo dargestellt ist, dass ein Access-Provider eine Anfrage bei einem DNS-Server-Betreiber startet. Diesbezüglich gibt es keinen Unterschied zwischen dynamischen DNS-Server und den DNS-Server, die die Zuordnung zwischen fester IP-Adresse und Domain-Namen speichern.
[917] Siehe zu Log-Files S. 178.

in Betracht kommen muss. Auf diese Prüfung soll jedoch verzichtet werden, da dies den Umfang dieser Arbeit erheblich erweitern würde..

Der Betreiber des dynamischen DNS-Servers ist dementsprechend gegenüber dem Inhaber des Ziel-Domain-Namens gemäß § 96 Abs. 2 TKG „nur" verpflichtet, die Zuordnung zwischen dynamischer IP-Adresse und festen Domain-Namen zu dem Zeitpunkt unverzüglich zu löschen, in welchem diesem eine neue dynamische IP-Adresse zugewiesen wird.[918]

ccc. Routerbetreiber

Routerbetreiber erbringen Telekommunikationsdienste und wirken als Betreiber von Telekommunikationsanlagen bei der Erbringung von Telekommunikationsdiensten/ Telekommunikationsdienstleistungen gemäß § 3 Nr. 6b) TKG mit.[919] Ohne ihre Mitwirkung würde die Telekommunikation im Internet nicht funktionieren. Betreiber von Telekommunikationsanlagen werden in den Kreis der zur Geheimhaltung des Fernmeldegeheimnisses Verpflichteten gemäß § 88 TKG mit einbezogen.[920] Auch sie müssen personenbezogene Daten schützen, soweit sie ihnen bekannt werden.

Fraglich ist, ob sie zur Löschung der jeweiligen IP-Adressen bzw. von erstellten Protokolldaten, die sich auf die Daten der einzelnen Verbindung beziehen, wie IP-Adressen, Datum, Uhrzeit, sowie darüber hinaus zur Löschung der IP-Pakete[921] verpflichtet sind, die über ihre Router weitervermittelt werden.

---

[918] Dies wird regelmäßig spätestens nach einen Zeitraum von 24 Stunden der Fall sein (vgl. Voss, Das große PC & Internet Lexikon 2007, S. 351).
[919] Vgl. insbesondere die Darstellung bei Köhntopp/Köhntopp, CR 2000, 248, 249. Zum Begriff des Routing siehe auch Koch, Internet Recht, S. 9. Zum Begriff des Routers siehe auch S. 31 sowie Petri/Göckel, CR 2002, 329, 333 Fn. 38 (Router heißt zu Deutsch Leitweglenkung, Wegefindung, Wegewahl. In paketorientierten Kommunikationssystemen bedeutet dies die Entscheidung von Vermittlungsknoten oder Routern, welchen Weg eine Datei oder ein Dateifragment nehmen soll, um zum Empfänger zu gelangen). Siehe außerdem S. 114/142/143 ff., wo unter anderem auch darauf verwiesen worden ist, dass unter den Begriff der Telekommunikationsanlagen nach § 3 Nr. 23 TKG die Server und Router zur Steuerung und Vermittlung von Online-Kommunikation fallen, siehe Büchner in: TKG-Kommentar, § 85 TKG Rn. 2; Bock in: TKG-Kommentar, § 88 TKG Rn. 11; Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 85 TKG(1998), Band 1, Rn. 11.
[920] Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 4; Bock in: TKG-Kommentar, § 88 TKG Rn. 25.
[921] Zur paketvermittelten Übertragung im Internet siehe etwa Sieber in Hoeren/Sieber, Teil 1 Rn. 45 ff. sowie S. 20 in dieser Arbeit.

(1) Tunnel-Startpunkt

Im Sinne der im zweiten Abschnitt aufgestellten These, dass allein eine **vollständige Anonymisierung gemäß § 3 Abs. 6 1. Alt. BDSG durch Löschung** von Daten und der entsprechenden Identifikationsmerkmale dem Grundsatz der Datenvermeidung optimal Rechnung tragen kann, muss auch hier grundsätzlich die Löschung der IP-Adresse im Vordergrund stehen.[922] Datenvermeidung lässt sich am besten bewerkstelligen, sofern Daten von vorneherein nicht längerfristig entstehen, und damit die Gefahr einer nachträglichen Herstellung des Personenbezugs ausgeschlossen ist.[923]

Diese für den Datenschutz wünschenswerte Vorgabe im Sinne einer „tatsächlich" effektiven Datenvermeidung und Datensparsamkeit lässt sich allerdings als Rechtspflicht gemäß § 96 Abs. 2 TKG für den Routerbetreiber wie folgt begründen:
Die IP-Adressen stellen im Rahmen von Routing Verkehrsdaten gemäß § 3 Nr. 30 TKG, § 96 Abs. 1 Nr. 1 TKG dar.[924]
Eine längerfristige Speicherung der IP-Adresse für Abrechnungszwecke gemäß § 97 Abs. 2 TKG ist für einen Routerbetreiber nicht erforderlich, da Summendaten über die transferierten Datenmengen gespeichert werden, anhand derer die Abrechnung erfolgt.[925] Für die Abrechnung ist lediglich notwendig, das Datenvolumen demjenigen Provider zuordnen zu können, mit welchem die Abrechnung erfolgt. Daher kann ein Verfahren eingesetzt werden, welches ermöglicht, ein entstandenes Datenvolumen eindeutig einem Provider zwecks Abrechnung zuzuweisen, ohne aber notwendigerweise die IP-Adressen der jeweiligen Nutzer längerfristig zu speichern.[926] Das grundsätzliche Recht,

[922] Siehe zur effektiven Datenvermeidung S. 106 ff.
[923] Vgl. zur frühestmöglichen Löschung auch Roßnagel in: Roßnagel, Handbuch Datenschutzrecht, 1 Rn. 40.
[924] Siehe zur IP-Adresse die Ausführungen auf S. 164 ff.
[925] Dies heißt auch, dass für eine Abrechnung lediglich die Speicherung der „anonymen" Datengesamtsumme notwendig ist (siehe hierzu auch Köhntopp/Köhntopp, CR 2000, 248, 251).
[926] Vgl. außerdem Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 121, der beim E-Mail-Anbieter darauf hinweist, dass der Diensteanbieter zwar auf der einen Seite sein Angebot aufrechterhalten und optimieren muss und nur in Kenntnis der Benutzungszeiten seiner Kunden in der Lage ist, die von ihm vorgehaltene Hardware für seine Dienstleistung zu optimieren und Engpässe zu vermeiden. Auf der anderen Seite reiche es jedoch aus, wenn der Anbieter den Zeitumfang und Datenmenge von einem beliebigen Kunden kenne, so dass die Anonymisierung des Datenbestandes geboten ist. Diese Überlegungen von Kleine-Voßbeck können entsprechend auf den Routerbetreiber im Rahmen seiner Abrechnung angewendet werden, da

das Datenvolumen für Abrechnungszwecke zu speichern, ergibt sich nunmehr außerdem ausdrücklich aus § 96 Abs. 1 Nr. 2 TKG.

Die IP-Adresse ist für den Routerbetreiber darüber hinaus nicht anonym. Anonym im Sinne der gesetzlichen Regelung des § 3 Abs. 6 BDSG bedeutet zwar nicht zwangsläufig, dass der Personenbezug für immer beseitigt ist, sondern nur, dass sich dieser schwer (d.h. mit einem unverhältnismäßigen großen Aufwand an Zeit, Kosten und Arbeitskraft) herstellen lässt.[927] Gerade im Internet ist aber einerseits Personenbezogenheit oder Anonymität aufgrund der Zusammenführungsmöglichkeiten der Daten sehr stark „momentbezogen".[928] Außerdem kann die Frage eines unverhältnismäßigen Aufwands nur in den Fällen im Vordergrund stehen, in denen die verarbeitende Stelle die alleinige datenverarbeitende Stelle darstellt und beispielsweise ein Anonymisierungsverfahren entwickelt hat, das die De-Anonymisierung nur mit großem Aufwand zulässt. Liegt ihr demnach keine Referenzliste mit Namen und Adressen der jeweiligen (anonymisierten) Personen vor, so ist die Wiederherstellbarkeit des Personenbezugs tatsächlich eine Frage der Wahrscheinlichkeit und des unverhältnismäßig großen Aufwands.
Beruht jedoch eine Re-Personalisierungsmöglichkeit allein darauf, dass zwei verarbeitende Stellen lediglich ihr Wissen austauschen und verknüpfen müssten, so geht die Frage nach dem unverhältnismäßigen Aufwand fehl. Denn der Wissensaustausch stellt für sich betrachtet einen einfachen Vorgang dar. Für den Routerbetreiber wäre es theoretisch und ohne unverhältnismäßig großen Aufwand möglich, beim Access-Provider den dazugehörigen Versender eines Datenpakets zu erfragen. Auf einem anderen Blatt stehen die Annahme, dass den Routerbetreiber diese Daten regelmäßig nicht interessieren werden, sowie die Unsicherheit, ob der Access-Provider bereit wäre, dieses Wissen zu offenbaren. Dennoch kann Anonymität nicht von subjektiven Interessen oder vom Zufall abhängen. Daher muss stets im Falle von zwei datenverarbeitenden Stellen gelten, dass keine Anonymität vorliegt, wenn eine Stelle Kenntnis über

auch hier die Erbringung der Dienstleistung ohne Speicherung von personenbezogenen Daten möglich ist.

[927] Vgl. Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 196.

[928] Siehe hierzu im Besonderen auch Schaar, Datenschutz im Internet, Rn. 174, der sich in seinem Ausführungen auf vielfältigen Möglichkeiten zur Zusammenführung personenbezogener Daten im Internet bezieht.

die personenbezogenen Daten bzw. die entsprechenden Identifizierungsmerkmale hat.
Ebenso wenig kann hier im Vordergrund stehen, ob das Zusatzwissen legal erworben werden kann. So wird die Auffassung vertreten, dass im Rahmen der personenbezogenen Daten bestimmbarkeitsrelevantes Wissen nur solches ist, welches auf legalem Wege erhältlich ist.[929] Dies kann jedoch in dieser Allgemeinheit nicht überzeugen, da es im Rahmen des Datenschutzes auf den tatsächlichen Vorgang ankommen muss. Anonymität kann nicht nur deswegen bejaht werden bzw. die Bestimmbarkeit einer Person nicht nur allein aus dem Grunde abgelehnt werden, weil das Wissen illegal erworben worden ist.[930] In diesem Falle kann nicht von (faktischer)[931] Anonymisierung gesprochen werden.

Außerdem ist auch hier § 3a BDSG zu beachten. Dessen Intention liegt ebenso darin, auf Gefährdungen des informationellen Selbstbestimmungsrechts unter den Bedingungen moderner Datenverarbeitung zu reagieren,[932] die unter anderem in der Gefährdung der Unübersichtlichkeit der Datenverarbeitung bei unterschiedlichen Stellen liegen können.[933]

Der Routerbetreiber wäre nur dann zur Speicherung der IP-Adresse berechtigt, sofern er diese entweder nachweisbar und nachprüfbar für Störungszwecke im Sinne von § 100 Abs. 1 TKG benötigt, oder der Access-Provider unverzüglich nach Verbindungsende seiner Verpflichtung gemäß § 96 Abs. 2 TKG nachkommt und die entstandenen Verkehrsdaten, insbesondere die IP-Adresse, unverzüglich löscht.[934]

---

[929] Vgl. Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 96.
[930] Siehe hierzu auch Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 37, der als zur Identifikation einer Person geeignetes Zusatzwissen solches Wissen einstuft, dessen legales Bekanntwerden nach sozialüblichen Maßstäben nicht ausgeschlossen werden kann. Dammann legt mit dieser Aussage nicht grundsätzlich fest, dass stets Legalität in Bezug auf den Wissenserwerb vorliegen muss oder musste, sondern gibt lediglich eine Richtlinie dahingehend vor, inwieweit die Bestimmbarkeit einer Person wahrscheinlich ist. Dies kann aber im Umkehrschluss nicht bedeuten, die Bestimmbarkeit einer Person dann zu verneinen, wenn im Einzelfall ein illegaler Wissenserwerb vorliegt.
[931] Siehe zur faktischen Anonymität Tinnefeld in: Roßnagel, Handbuch Datenschutzrecht, 4.1 Rn. 24.
[932] Siehe Bizer in: Simitis, BDSG-Kommentar, § 3a BDSG Rn. 9.
[933] Vgl. Bizer in: Simitis, BDSG-Kommentar, § 3a BDSG Rn. 21.
[934] Vgl. hierzu die Ausführungen auf S. 162 ff.

In diesem Falle ist der Personenbezug der IP-Adresse bereits vollständig gemäß § 3 Abs. 6 1. Alt. BDSG (durch den Access-Provider) beseitigt worden, was allerdings ausnahmslos nur dann gelten kann, sofern der Access-Provider dynamische IP-Adressen vergeben hat.

In Bezug auf die Praxis ist anzumerken, dass die Routerbetreiber derzeit ohnehin sämtliche Verkehrsdaten unverzüglich löschen, da ansonsten die Speicherkapazitäten überlastet wären.[935]

(2) Verschlüsselung

Fraglich ist allerdings bei einem VPN, ob bei Verwendung von IPSec und dem Austausch des IP-Headers der Personenbezug der IP-Adresse des Tunnel-Startpunkts und der IP-Adresse des Tunnel-Endpunkts vollständig ausgeschlossen bzw. beseitigt werden könnte.[936] Dies hätte zur Folge, dass bereits nutzerseitig durch die Verwendung von entsprechender Technik etwas für die Sicherstellung „seines Datenschutzes“ getan werden könnte.[937]
So ist es mittels eines speziellen von IPSec verwendeten Protokolls möglich, den ursprünglichen IP-Header zu verschlüsseln.[938]

---

[935] Siehe zur EU-Richtlinie, die neue Speicherungsfristen im Sinne einer Vorratsdatenspeicherung regelt, S. 175 ff.
[936] Siehe zu IPSec S. 39 ff.
[937] Siehe zu den Möglichkeiten des Selbstdatenschutzes Bizer in: Simitis, BDSG-Kommentar, § 3a BDSG Rn. 26.
[938] Siehe zur Einfügung eines neuen IP-Headers S. 42. Vgl. zum speziellen Protokoll ESP (Encapsulating Security Payload), welches den ursprünglichen IP-Header verschlüsselt, Lipp, VPN, S. 209 ff.; Davis, IPSec, S. 211 ff. So schafft IPSec die Möglichkeit, das komplette IP-Datenpaket in ein zweites IP-Datenpaket zu verkapseln, so dass auch die Adressen, verwendeten Protokolle, die ebenfalls Verkehrsdaten darstellen und daher eigentlich zu löschen wären, nicht mehr sichtbar sind (siehe S. 42 ff. und Lipp, VPN, S. 190). Es kann lediglich noch die Gesamtmenge an Paketen ermittelt werden, die über das Internet versendet werden (Lipp, VPN, S. 190). Hier könnte gegebenenfalls auch ein „Umsteigebahnhof“ in Gestalt eines zusätzlichen, seitens des Providers betriebenen Servers eingesetzt werden, so dass die Verkehrsbeziehungen vollumfänglich verdeckt wären (siehe auch Schneider, MMR 1999, 571, 575, der einen zusätzlichen Server als „Umsteigebahnhof“ bezeichnet und Bedenken dagegen äußert, dass auf diese Art und Weise auch rechtlich bedenkliche Inhalte unerkannt über das Internet versendet werden können). Sofern der Provider den Gateway mit einer auf ihn selbst eingetragenen IP-Adresse mehreren Kunden zur Verfügung stellt (über diesen Server also Datentransfer von mehreren Personen abgewickelt werden), könnte ein (unberechtigter) Dritter noch nicht einmal mehr das jeweilige gesendete Datenvolumen nachvollziehen. In einem solchen Falle kann der Datenstrom nicht mehr verfolgt werden, und zwar weder, wer mit wem kommuniziert hat, oder das jeweilige Datenvolumen noch aufgrund der Datenverschlüsselung der jeweilige Dateninhalt.

Zu berücksichtigen ist aber, dass zwar der IP-Header verschlüsselt wird, aber der neue IP-Header ebenso einem Gateway oder einem Server zuordbar sein muss, da anderenfalls die Datenpakete nicht versandt und nicht zugestellt werden können.[939]

Sofern der neue IP-Header daher auf den VPN-Auftraggeber am Tunnel-Startpunkt oder Tunnel-Endpunkt schließen lässt, ist keine Anonymisierung eingetreten. Es lässt sich allenfalls eine Pseudonymisierung gemäß § 3 Abs. 6a BDSG dadurch erreichen, dass die neue IP-Adresse auf den Access-Provider lautet und einem von ihm betreuten Gateway zuzuordnen ist, wie beispielsweise im oben dargestellten Falle des Komplettmanagement des Gateways.[940] Der VPN-Auftraggeber würde dann nicht mehr in Erscheinung treten, sofern sowohl am Tunnel-Startpunkt als auch am Tunnel-Endpunkt Gateways eingesetzt werden, die beide dem Provider des VPN zuzuordnen wären.[941]

Der VPN-Auftraggeber ist aber in diesem Falle zumindest im Verhältnis zu potenziellen Angreifern oder Hackern besser geschützt. Denn bei Einsatz eines vom Provider betriebenen Gateway sowohl am Tunnel-Startpunkt als auch am Tunnel-Endpunkt nebst Austausch von IP-Adressen, ist für einen Dritten lediglich erkennbar, dass der Provider kommuniziert.

Damit können Datenspuren insoweit vermieden werden, dass für Dritte nicht mehr nachvollziehbar ist, wer tatsächlich an dem Telekommunikationsvorgang beteiligt ist. Dadurch wird also die Übertragung von Daten „datenschutzfreundlicher“ gestaltet[942]

[939] Siehe Davis, IPSec, S. 204/208, der ausführt, dass Router, die Pakete zu ihrem Bestimmungsort lenken, gewisse Informationen im IP-Header benötigen, wobei die neuen IP-Header, die an die Datenpakete eingefügt werden, für Router lesbar sind, aber die inneren IP-Header geschützt sind. Dies wird auch aus dem Grunde durchgeführt, um die privaten Netzwerkadressen zu schützen und für Dritte nicht lesbar zu gestalten.

[940] Siehe zum Komplettmanagement des Gateways durch den Provider S. 49. Vgl. hierzu auch Schaar, Datenschutz im Internet, Rn. 163, der ausführt, dass öffentliche Schlüssel, die vom Nutzer durch Verwendung von geeigneter Software erzeugt werden, zu den selbst erzeugten Pseudonymen gehören (Schaar (aaO) bezeichnet diese auch als Referenz-Pseudonyme, da üblicherweise das Pseudonym durch eine vertrauenswürdige Instanz zertifiziert wird, die Kenntnis von der Identität des Träger hat.).

[941] Siehe hierzu das Beispiel auf S. 44, in welchem sowohl Zweigstelle als auch Firmenzentrale mit einem Gateway ausgerüstet sind. Siehe zum Komplettmanagement des Gateways durch den Provider außerdem S. 49.

[942] Siehe hierzu auch S. 108 ff.

Im Hinblick auf den Inhalt der Datenpakete wird zwar regelmäßig die „Zerstückelung“ der Nachricht, keinen sinnvollen Einblick in personenbezogene Daten ermöglichen.[943] Da aber der Routerbetreiber hier ebenso wenig ein Interesse an der Speicherung des Datenpakets hat, gelten die Ausführungen zur Löschung der IP-Adresse beim Routing entsprechend, und es muss hier eine Löschung der (Inhalts-)Daten erfolgen.[944] Der Routerbetreiber ist als Telekommunikationsdiensteanbieter darüber hinaus gemäß § 88 Abs. 2 TKG zur Wahrung des Fernmeldegeheimnisses verpflichtet.

Aus Sicht der Praxis gilt bereits zum jetzigen Zeitpunkt, dass aufgrund der Kapazitätsengpässe regelmäßig keine Dateninhalte auf den Routern gespeichert werden. Dennoch soll die grundsätzliche Möglichkeit untersucht werden, da gezeigt werden soll, wo „überall“ Daten anfallen und nach welchen gesetzlichen Regelungen verarbeitet werden. Denn insbesondere für Strafverfolgungsbehörden eröffnen sich unterschiedliche Möglichkeiten, wobei deren Maßnahmen aber stets im Einklang mit den entsprechenden gesetzlichen Vorschriften stehen müssen.[945]

[943] Siehe zur paketvermittelten Übertragung im Internet außerdem Fn. 8. Aber auch in einer Teilinformation kann grundsätzlich etwas enthalten sein, was der Geheimhaltung unterliegt (wie etwa Betriebs- oder Geschäftsgeheimnisse oder personenbezogene Daten, die nach dem BDSG zu schützen wären). Der Inhalt der Nachricht ist zwar in verschiedene Datenpakete aufgeteilt, die über verschiedene Routen laufen, und die erst am Zielort wieder zusammengefügt werden, dennoch kann auch für ein einzelnes Datenpaket gleichermaßen ein Geheimhaltungsbedürfnis des Absenders in Betracht kommen.

[944] Siehe auch Freytag, Haftung im Netz, S, 224, der ausführt, dass Router Datenpakete von einem Teil des Netzes in den nächsten weiterleiten und sie zwischenspeichern (cache), solange keine Leitung frei ist, wobei aber die Inhalte nicht im Klartext erscheinen, sondern nach dem TCP-Protokoll verschlüsselt. Hier ist missverständlich, dass eine Verschlüsselung nach dem TCP-Protokoll vorliegen soll. Denn dieses stellt kein Verschlüsselungsprotokoll, sondern ein Übertragungsprotokoll dar (siehe zu TCP/IP S. 20), zudem wird der Begriff „Klartext“ grundsätzlich im Zusammenhang mit „Kryptographie“ verwendet (Tanenbaum, Computernetzwerke, S. 783). Siehe außerdem die vorherige Fn. 943 und die Auffassung von Spindler, der von der Lesbarkeit des Inhalts ausgeht, wobei lediglich die Zerstückelung problematisch ist.

[945] Siehe zur EU-Richtlinie, die neue Speicherungsfristen im Sinne einer Vorratsdatenspeicherung regelt, S. 175 ff.

bb. Technische Schutzmaßnahmen

Die Regelungen des TKG unterscheiden bei den datenschutzrechtlichen Pflichten nicht zwischen den Mitwirkenden und den Anbietern selbst.[946]
§ 88 Abs. 2 TKG normiert klar, dass auch diejenigen zur Wahrung des Fernmeldegeheimnisses verpflichtet sind, die an der geschäftsmäßigen Erbringung von Telekommunikationsdiensten gemäß § 3 Nr. 6 b) TKG mitwirken.
Da aber Routerbetreiber und DNS-Server-Betreiber in keinerlei Beziehung zu dem Nutzer stehen, können datenschutzrechtliche Pflichten nur eingeschränkt gelten. Es wäre es für die Routerbetreiber und DNS-Server-Betreiber praktisch unmöglich, eine Einwilligung im Sinne von § 4a BDSG[947] zur Verarbeitung personenbezogener Daten einholen, da sie mit den entsprechenden Teilnehmern bzw. Nutzern in keinerlei Kontakt stehen. Entsprechendes gilt etwa für die Unterrichtungspflicht nach § 93 TKG.
Somit sind diese datenschutzrechtlichen Regelungen von vorneherein für Routerbetreiber und DNS-Server-Betreiber in der Praxis schwer umsetzbar.[948]
Diese Verpflichtungen können und müssen von dem Access-Provider wahrgenommen werden, der in unmittelbarem Kontakt zu den Teilnehmern steht.

Dadurch sind aber Routerbetreiber und DNS-Server-Betreiber nicht von etwaigen Sorgfaltspflichten befreit. So obliegt nach § 109 Abs. 2 TKG den Betreibern von Telekommunikationsanlagen, wozu die Betreiber von Router und DNS-Servern zählen,[949] die technische Verpflichtung den betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen

[946] Vgl. § 3 Nr. 6 TKG, § 91 Abs. 1 TKG.
[947] Vgl. zur elektronischen Einwilligung auch § 94 TKG.
[948] Insbesondere Betreiber von Routern wissen im Vorhinein noch nicht einmal, welche Datenpakete von welchen Nutzern sie transportieren. Siehe hierzu auch das Beispiel von Campo/Pohlmann, Virtual Private Networks, S. 59/60. Hier wird anschaulich dargestellt, welchen Weg IP-Pakete zurücklegen können, die zwischen zwei Kommunikationspartner ausgetauscht werden, die nur 3 km weit entfernt voneinander liegen. Hierbei sind 23 Router beteiligt, die auch außerhalb Deutschlands angesiedelt sind. Die Verfasser verweisen ebenfalls darauf, dass abhängig von dem jeweiligen Provider manche IP-Pakete sogar bei kurzen Strecken über die USA geroutet werden.
[949] Siehe zur Telekommunikationsanlage S. 114/142/143 sowie Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 2; Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 11

Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und von Telekommunikations- und Datenverarbeitungssystemen
gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen.[950]
Zu berücksichtigen ist hierbei vor allem, dass von einem Routerbetreiber nicht der Einsatz von Verschlüsselungsprogrammen erwartet werden kann, da vielmehr der Nutzer bzw. der Teilnehmer selbst angehalten ist, entsprechende Verschlüsselungen einzusetzen.[951]

Entsprechendes gilt für den TK-Provider, da auch dieser nicht in der Lage ist, die Daten zu verschlüsseln. Soweit er aber die Funktion des Access-Providers wahrnimmt, ist er in dieser Funktion zur Aufklärung über Verschlüsselungsmaßnahmen verpflichtet.

cc. Auskunfts- und Überwachungsmaßnahmen

Im Hinblick auf DNS-Betreiber gilt, dass diese zwar wie oben festgestellt an der Erbringung eines Telekommunikationsdienstes mitwirken und dass es sich bei einem DNS-Server auch um eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG handelt.[952] Dennoch muss hier berücksichtigt werden, dass Access und DNS untrennbar miteinander verbunden sind, da ohne DNS der Access nicht funktionieren würde und ohne Access die DNS-Leistung überflüssig wäre.[953] Sofern also ein Access-Provider gemäß § 3 Abs. 2 Nr. 2 TKÜV von der Vorhaltung von vorbereitenden organisatorischen Vorkehrungen befreit ist,[954] muss dies auch für den DNS-Server gelten und – da diesbezüglich keine andere rechtliche Bewertung gerechtfertigt ist – für den Betreiber eines Routers, der ebenso „nur“ an der Erbringung eines Telekommunikationsdienstes gemäß § 3 Nr. 6 b) TKG mitwirkt.[955]

[950] Vgl. hierzu, insbesondere zum Umfang der Schutzmaßnahmen und den Möglichkeiten der Bundesnetzagentur, gemäß § 115 Abs. 3 TKG die obigen Ausführungen auf S. 200 . Siehe außerdem Röhrborn/Katko, CR 2002, 882, 887; Gola/Klug, Grundzüge des Datenschutzrechts, S. 199.
[951] Siehe hierzu bereits die Ausführungen zum Access-Providing auf S. 196 ff.
[952] Siehe S. 141 ff.
[953] Siehe S. 141.
[954] Siehe S. 200.
[955] Siehe S. 143ff.

TK-Provider fallen allerdings nicht unter den Ausnahmetatbestand des § 2 Abs. 3 Nr. 3 TKÜV.

Irreführend sind jedoch insoweit die Ausführungen der Bundesnetzagentur dahingehend, dass Internet-Access via DSL oder Festverbindung (Standleitung), nicht von der Befreiung nach § 3 Abs. 2 Nr. 3 TKÜV betroffen sind, da die Verpflichteten entsprechende vorbereitende technische Maßnahmen bezüglich des Übertragungsweges vorhalten könnten.[956] Die Bundesnetzagentur geht also davon aus, dass es sich bei DSL-Technik und Festverbindung um einen unmittelbaren Internet-Zugang mit der grundsätzlichen Möglichkeit der Anbieter handelt, am Übertragungsweg die entsprechenden Vorkehrungen zu treffen. Hierbei wird allerdings nicht berücksichtigt, dass ein Anbieter von DSL nicht zwangsläufig Betreiber des Übertragungsweges ist, da es sich bei DSL lediglich um eine Technologie unter Inanspruchnahme des Telefonnetzes handelt.[957] Entsprechendes gilt für die Anbieter einer Standleitung, sofern damit einem Kunden lediglich fest definierte Bandbreiten bzw. Übertragungskapazitäten zur Verfügung gestellt werden.[958] Dies bedeutet, dass ein Anbieter nicht notwendigerweise über den zugrundeliegenden Übertragungsweg, die Teilnehmeranschlussleitung und/oder ein Backbone verfügen muss.[959] So gibt es ebenso so genannte virtuelle Providerohne eigene Infrastruktur, die DSL anbieten.[960] DSL ist grundsätzlich nicht anders zu bewerten als ein Internetzugang über eine Wählverbindung. Der einzige Unterschied besteht darin, dass in der

[956] Siehe hierzu auch den Download unter http://www.bundesnetzagentur.de/enid/78f203c9cbedb13a969685e262e885f3,55a304092d09/Technische_Regulierung_Telekommunikation/Technische_Umsetzung_von_Ueberwachungsma_nahmen_h6.html und die dortigen Ausführungen zu „Vorläufiges Verfahren zur technischen Umsetzung von Maßnahmen zur Überwachung der Telekommunikation bei unmittelbaren Internet-Zugängen" (Website vom 30.09.2006). Vgl. außerdem die Ausführungen des Bundesbeauftragten für den Datenschutz „Begründung zum Entwurf einer Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV), abrufbar unter www.bfd.bund.de/information/symp2_ulrich3.html (Website vom 01.08.2004), dass Internet-Access via DSL oder Festverbindung (Standleitung), nicht von der Befreiung nach § 3 Abs. 2 Nr. 3 TKÜV betroffen sind, da die Verpflichteten entsprechende vorbereitende technische Maßnahmen bezüglich des Übertragungsweges vorhalten könnten.

[957] Siehe oben S. 29/29.

[958] Vgl. hierzu auch die an die Bundesnetzagentur übersandte Stellungnahme der BT (Germany) GmbH & Co. oHG vom 09.01.2004, S. 4, abrufbar unter http://www.bundesnetzagentur.de/media/archive/520.pdf (Website vom 30.09.2006).

[959] Siehe auch S. 25 ff. in dieser Arbeit.

[960] Vgl. zu diesem Begriff S. 25 ff. sowie Summa in: Holznagel/Nelles/Sokol, TKÜV, S. 25)

Vermittlungsstelle ein so genannter Splitter eingesetzt wird,[961] der zwischen Sprache und Datenpaketen trennt. Hiervon zu unterscheiden ist aber die Frage, ob der DSL-Anbieter ebenso Betreiber des Übertragungsweges bzw. der Teilnehmeranschlussleitung gemäß § 3 Nr. 28 TKG ist.[962] Denn insbesondere wird der Anschluss des Teilnehmers weiterhin einem TK-Anbieter bereit gestellt, und ein DSL-Anbieter erhält nur die Möglichkeit, die Leitung für seine Datenübertragung zu nutzen.[963] Die Teilnehmeranschlussleitung kann weiterhin von einem TK-Provider betrieben, insbesondere weiterhin auch für ihre Sprachtelefondienste genutzt werden. Durch einen DSL-Splitter wird nur die Möglichkeit geschaffen, die vorhandenen Kanäle der Teilnehmeranschlussleitung in einen Sprachkanal und zwei Datenübertragungskanäle aufzusplitten, die getrennt genutzt werden können.[964] Daher muss konsequenterweise die Vorhaltung von Überwachungsmaßnahmen an den Betrieb eines Übertragungsweges und nicht an die zugrundeliegende Technologie geknüpft werden, die über diesen Übertragungsweg bereitgestellt wird. Dies bedeutet, dass nicht das Angebot von DSL oder vergleichbaren Diensten bzw. von einer Standleitung der ausschlaggebende Punkt für die Bereitstellung der Überwachungsmaßnahme sein kann, sondern die Funktionsherrschaft über den Übertragungsweg.[965]

Im Hinblick auf Auskunftspflichten gemäß § 113 Abs. 1 TKG gilt für DNS-Betreiber und Routerbetreiber (anders als für TK-Provider), dass sie kein eigenes Vertragsverhältnis mit dem Teilnehmer oder Nutzer eingehen, so dass sie auch grundsätzlich keine Auskünfte über die nach den §§ 93 und 109 TKG erhobenen Daten erteilen können.

[961] Vgl. Tanenbaum, Computernetzwerke, S. 157.
[962] Siehe hierzu auch § 6 TKG sowie die Ausführungen auf S. 26 Fn. 93.
[963] Vgl. Voss, Das große PC & Internet Lexikon 2007, „DSL“ S.257.
[964] Siehe Kath/Riechert, Internet-Vertragsrecht, Rn. 52. Line Sharing oder Kanalteilung führt nicht zur Einstufung als Betreiber eines Übertragungsweges, sofern nur Kanäle an Dritte weitervermietet werden, siehe hierzu Schütz in: TKG-Kommentar (2. Auflage), § 6 TKG Rn. 19.
[965] Vgl. zur Funktionsherrschaft Schütz in: TKG-Kommentar, § 6 TKG Rn. 33; Piepenbrock/Attendorn in: TKG-Kommentar (3. Auflage), § 16 TKG Rn. 23 ff.

dd. Zwischenergebnis

Der Access-Provider ist gemäß § 96 Abs. 2 TKG zur unverzüglichen Löschung der dynamischen IP-Adresse nach jedem Verbindungsvorgang verpflichtet, während er die von ihm vergebene statische IP-Adresse als ein zum Aufbau weiterer Verbindungen notwendiges Datum speichern darf. Bei der Frage der „unverzüglichen Löschung“ ist allerdings der für die Zwecke der §§ 97 ff. notwendige Zeitraum zu berücksichtigen.[966]
Bei Einordnung des Access-Providing als Teledienst und der damit verbundenen Anwendbarkeit des TDDSG wäre der Access-Provider nicht zur Löschung der Tunnel-Startpunkte und Tunnel-Endpunkte verpflichtet, wenn es sich bei dem VPN-Auftraggeber um eine juristische Person oder Personengesellschaft handelt. Insbesondere wäre der Access-Provider nicht für die Maßnahmen gemäß §§ 88, 109 TKG, also weder zur Wahrung des Fernmeldegeheimnisses gemäß § 88 TKG, zur Aufklärung über Verschlüsselungsmaßnahmen noch für die technischen Schutzmaßnahmen gemäß § 109 Abs. 2 TKG verantwortlich.

Der TK-Anbieter muss die Anschlussnummer gemäß § 96 Abs. 2 TKG unverzüglich löschen, sofern er diese nicht für seine Abrechnungszwecke benötigt. Außerdem darf er die Zielnummer lediglich dann ungekürzt gemäß § 97 Abs. 4 Nr. 1 TKG speichern, sofern sein Kunde bzw. der Teilnehmer nicht die Kürzung um die letzten drei Ziffern oder die vollständige Löschung verlangt.

Der DNS-Server-Betreiber ist zur Speicherung der Zuordnung zwischen fester IP-Adresse und Domain gemäß § 28 Abs. 1 Nr. 1 BDSG berechtigt, muss diese aber nach § 35 Abs. 2 BGB löschen. Bei juristischen Personen oder Personengesellschaften, für die das BDSG keine Anwendung findet, kann sich daher eine vertragliche Pflicht zur Löschung empfehlen. Beim dynamischen DNS-Verfahren muss der DNS-Server-Betreiber gemäß § 96 Abs. 2 TKG jedoch die Zuordnung einer dynamischen IP-Adresse zu einem festen Domain-

[966] Siehe S. 170 ff. Siehe zur Erforderlichkeit einer Datenverarbeitung auch S. 98.

Namen nach jedem Verbindungsvorgang unverzüglich löschen, in der Regel also nach 24 Stunden.[967]

Der Routerbetreiber ist gemäß § 96 Abs. 2 TKG zur unverzüglichen Löschung der IP-Adressen und des Inhalts der Datenpakete verpflichtet. Denn diesbezüglich ist insbesondere zu berücksichtigen, dass der Routerbetreiber diese Daten nicht für seine weitere Diensterbringung benötigt. Das Datenvolumen darf er für Zwecke seine Abrechnung gemäß § 96 Abs. 1 Nr. 2 TKG grundsätzlich erheben.

Bei einem VPN ist zusätzlich zu beachten, dass der Access-Provider an mehreren Standorten des VPN vertreten sein kann. Dennoch ist zwischen Tunnel-Startpunkten und Tunnel-Endpunkten zu trennen. Die feste bzw. statische IP-Adresse des Tunnel-Endpunkts ist aus Sicht desjenigen, der am Tunnel-Startpunkt den Internetzugang bereitstellt, gemäß § 96 Abs. 2 TKG zu löschen, während sie am Tunnel-Startpunkt für Zwecke des Verbindungsaufbaus ständig gespeichert werden darf. Sofern es sich hierbei im Rahmen eines VPN an den unterschiedlichen Standorten bzw. Tunnel-Startpunkten und Tunnel-Endpunkten um ein und denselben Provider handelt, hat dies insoweit Bedeutung, sofern unterschiedliche Systeme bzw. Geräte eingesetzt werden, bei denen unterschiedliche Daten anfallen und die sämtlich darauf auszurichten sind, so wenig wie möglich personenbezogene Daten zu erheben. Denn so ist es im Sinne eines effektiven Systemdatenschutzes gemäß § 3a BDSG beispielsweise erforderlich, bei den Geräten, die lediglich für die Erbringung des Internetzugangs eingesetzt werden, die Ziel-IP-Adresse unverzüglich zu löschen.

Als rechtspolitisches Fazit kann für diesen Prüfungsteil darüber hinaus festgehalten werden, dass die geplante Einführung gesetzlicher Mindestspeicherungspflichten durch eigenverantwortliches und datenschutzgerechtes Handeln der Provider (was jederzeit durch Datenschutzaufsichtsbehörden überprüfbar ist) vermieden werden könnte.

---

[967] Vgl. Voss, Das große PC & Internet Lexikon 2007, „Flatrate“ S. 351.

2. Zwangsweises Tunneling und Datenvermeidung

a. Anwendbarkeit des BDSG

Beim zwangsweisen Tunneling steht die langfristige Speicherung der Zuordnung zwischen bestimmten Kennungen/personenbezogenen Informationen und der statischen IP-Adresse oder dem Domain-Namen[968] eines Unternehmens beim Provider in einer Datenbank im Vordergrund.[969] Auf diese Datenbank greift der Internetzugangsknoten (PoP) zu, um die Datenanfrage eines Unternehmensstandortes zu einem bestimmten (Unternehmens-) Gateway weiterzuleiten.
Hierfür kann der Provider etwa Benutzernamen und Passwörter, Einwahlnummern oder auch so genannte Präfixe/Suffixe mit der IP-Adresse oder dem Domain-Namen des Unternehmensstandorts verknüpfen.[970] Diesbezüglich kann ein Vergleich zu dem DNS-Service gezogen werden, da auch hier der Access-Provider auf bestimmte Informationen zurückgreifen muss, um die Kommunikation sicherzustellen, so dass es sich insgesamt um ein Verfahren handelt, welches an der Erbringung eines Telekommunikationsdienstes mitwirkt.[971]

Auf einem technischen System, dem Internetzugangsknoten bzw. der Datenbank, auf die der Internetzugangsknoten Zugriff nimmt, werden demgemäß personenbezogene Daten miteinander verknüpft. Das TKG enthält zur Frage der Zulässigkeit dieser Datenverknüpfung allerdings keine speziellen Regelungen.[972] Insbesondere erhebt und verwendet[973] der Provider keine Bestandsdaten gemäß § 95 TKG, da keine Grunddaten des Vertragsverhältnisses gemäß § 3 Nr. 3 TKG erhoben werden. Gemäß dieser Vorschrift sind Bestandsdaten die Daten eines Teilnehmers, die für die

[968] Sofern keine statische IP-Adresse vorhanden ist, müssen so genannte dynamische DNS-Server eingesetzt werden, die aufgrund eines Domain-Namens die Daten zu dem jeweiligen Unternehmen weiterleiten, siehe hierzu auch oben S. 56.
[969] Zur Erklärung des zwangsweisen Tunneling siehe S. 57 ff.
[970] Siehe S. 57 ff.
[971] Siehe S. 141.
[972] Vgl. oben S. 207 ff.
[973] Siehe zum Begriff des Verwendens Büttgen in: TKG-Kommentar (3. Auflage), § 95 TKG Rn. 7: Der Regelungsumfang der Vorschrift betrifft die Erhebung, Verarbeitung und Nutzung personenbezogener Daten i.S.d. § 3 Abs. 3, 4, 5 BDSG.

Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Die Definition des „Erheben“ findet sich in § 3 Abs. 3 BDSG und beinhaltet das Beschaffen von Daten über den Betroffenen. Dies bedeutet dementsprechend das Beschaffen über bereits existierende Daten als so genannte Vorphase, wobei etwa auch ein Erfragen von Daten in Betracht kommt.[974] Die Verknüpfung der personenbezogenen Daten stellt allerdings kein Erfragen oder Beschaffen, sondern vielmehr ein „Erschaffen“ dar. Insbesondere werden keine personenbezogenen Daten für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erfragt. Daher handelt es sich bei der Vergabe von Kennungen und deren Verknüpfung mit anderen Unternehmensdaten nicht um eine Datenerhebung gemäß § 3 Nr. 3 TKG, § 3 Abs. 3 BDSG.[975]
Zu berücksichtigen ist zwar, dass etwa der Domain-Name, mit dem die Kennung verknüpft wird, ein Bestandsdatum gemäß § 3 Nr. 3 TKG darstellen kann, sofern diese als Grunddaten des Vertragsverhältnisses erhoben worden sind.[976] Aber die Zulässigkeit der Verknüpfung der Daten auf diesem technischen System im Rahmen des zwangsweisen Tunneling ist an den Voraussetzungen des § 28 Abs. 1 BDSG zu messen, sofern der Kunde nicht ausdrücklich in die Verwendung der Daten zu diesem Zweck gemäß § 4a BDSG eingewilligt hat.

Die datenschutzrechtlichen Pflichten sind bezüglich der Herstellung dieser verknüpften Daten also gesondert zu betrachten. Dies ändert jedoch nichts an dem Umstand, dass die Einzeldaten „IP-Adresse“ oder „Domain-Name“, soweit diese an anderer Stelle oder auf einem anderen technischen System (d.h. in einem anderen Zusammenhang) nochmals gespeichert werden, anderen

[974] Vgl. Gola/Schomerus, BDSG, § 3 BDSG Rn. 24; vgl. auch Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 101 ff.; siehe außerdem zum „Erheben“ die Ausführungen auf S. 169 ff.
[975] Auch hier gilt, dass die Kennungen sowie IP-Adresse oder der Domain-Name personenbezogen sind, da sie sich auf ein bestimmtes Unternehmen beziehen (siehe hierzu ob S. 164 ff.), es sich aber dennoch in diesem Zusammenhang nicht um Bestandsdaten nach § 3 Nr. 3 TKG handelt. Diesbezüglich wird ebenso auf die Ausführungen zu der der statischen IP-Adresse und deren Ablehnung als Bestandsdatum verwiesen (S. 168 ff.).
[976] Vgl. zu den Grunddaten eines Vertragsverhältnisses S. 98. Siehe außerdem Büchner in: TKG-Kommentar (2. Auflage), § 4 TDSV (Anh § 89 TKG) Rn. 1, der ausführt, dass mit Bestandsdaten hauptsächlich Name und Anschrift des Kunden, Art des kontrahierten Dienstes sowie die dem Kunden zum Gebrauch überlassenen Einrichtungen gemeint sind. In diesem Sinne ebenso Janik/Büttgen in: TKG-Kommentar (3. Auflage), § 3 TKG Rn. 13.

datenschutzrechtlichen Regelungen oder Löschungspflichten, wie beispielsweise § 95 Abs. 3 TKG unterliegen können.
Welche gesetzliche Regelung anwendbar ist, hängt demnach von der konkreten Verwendung der Daten ab.
Daraus ergibt sich auch, dass der Vorgang der Verknüpfung zwischen den Kennungen und dem Domain-Namen eines Unternehmensstandortes im Hinblick auf juristische Personen ohne weiteres zulässig ist, da das BDSG hier gemäß § 1 Abs. 1 BDSG keine Anwendung findet.

Für natürliche Personen kann dahingegen die Zulässigkeit der Datenverarbeitung gemäß § 28 Abs. 1 Nr. 1 BDSG aus dem Grunde bejaht werden, da im Rahmen des zwangsweisen Tunneling gleichermaßen eine Speicherung gemäß § 3 Abs. 4 Nr. 1 BDSG und Verknüpfung von Kennungen durch den Provider, die der Authentifizierung dienen,[977] nur Mittel zum Zweck sind.[978] So wird sichergestellt, dass der Datenaustausch lediglich zwischen hierzu legitimierten (Unternehmens-) Standorten oder Nutzern in Betracht kommt.[979] Kontrollbefugnis und Löschungspflichten richten sich im Hinblick auf die datenschutzrechtlichen Pflichten natürlicher Personen nach §§ 34 ff. BDSG.

Der Provider ist allerdings nach Vertragsende nicht zwangsläufig zur Löschung gemäß § 35 Abs. 2 Nr. 3 BDSG der verknüpften Daten verpflichtet, sofern er die Daten noch für weitere Zwecke benötigen würde, was stets Frage des Einzelfalls ist.[980] Insbesondere ergibt sich, wie oben bereits ausgeführt, mit Ablauf des auf die Beendigung folgenden Kalenderjahres keine Löschungspflicht aus § 95 Abs. 3 TKG bezüglich der verknüpften Daten, so dass auch im Hinblick auf juristische Personen insoweit keine ausdrücklich gesetzlich normierte Löschungspflicht besteht.[981]

[977] Vgl. Lipp, VPN, S. 286 ff., der darlegt, dass beim zwangsweisen Tunneling der PoP bzw. die implementierte Datenbank einen Teil der Authentifizierung vornimmt.
[978] Siehe auch Simitis in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 79, der § 28 Abs. 1 Nr. 1 BDSG bejaht, sofern die Datenverarbeitung mit Rücksicht auf den Zweck eines zwischen der verantwortlichen Stelle und den Betroffenen bestehenden Vertragsverhältnisses benötigt wird.
[979] Siehe Lipp, VPN, S. 178/182.
[980] Gola/Schomerus, BDSG, § 35 BDSG Rn. 13, wobei jedoch regelmäßig von einer Löschungsverpflichtung auszugehen ist (vgl. auch Fn. 738).
[981] Siehe zu den Löschungsfristen von Bestandsdaten auch Büchner in: TKG-Kommentar (2. Auflage), § 4 TDSV (Anh § 89 TKG)Rn. 5;Büttgen in: TKG-Kommentar (3. Auflage), § 95 TKG Rn. 24-26.

Der als Bestandsdatum (bereits) erfasste Domain-Name darf gemäß § 95 Abs. 3 TKG bis zum Ablaufe des auf die Beendigung folgenden Kalenderjahres unter Umständen in einem anderen Zusammenhang und auf einem Datenträger gespeichert werden. Aber die Aufhebung der Verknüpfung des Domain-Namens mit besonderen Kennungen auf dem technischen System richtet sich nach § 35 Abs. 2 BDSG, wobei § 35 Abs. 2 Nr. 3 BDSG besondere Relevanz erhält. Gemäß dieser Regelung ist im Einzelfall stets zu prüfen, ob die weitere Speicherung der Daten unbedingt für (andere) vertragliche Zwecke notwendig ist.[982]

Eine juristische Person oder Personengesellschaft, für die das BDSG keine Anwendnung findet, sollte dementsprechend bei den Vertragsbestimmungen darauf achten, dass dort entsprechende Löschungspflichten geregelt sind.

b. Verkehrsdaten

Davon unabhängig zu betrachten ist dennoch, dass es sich bei der IP-Adresse oder Domain des Unternehmensstandorts sowie bei Benutzernamen, Einwahlnummer oder Präfix/Suffix „auch" um Verkehrsdaten gemäß § 3 Nr. 30 TKG handelt, da sie „bei" jedem Telekommunikationsvorgang im Sinne des zwangsweisen Tunneling erneut genutzt werden (müssen).[983] Diese Daten fallen bei jedem Vorgang des zwangsweisen Tunneling neben Datum und Uhrzeit der Verbindung an, so dass diese auf die jeweilige Verbindung bezogenen Einzelangaben (Logdaten) gemäß § 96 Abs. 2 TKG unverzüglich nach Ende der Verbindung zu löschen sind. Dies gilt auch im Hinblick auf juristische Personen und Personengemeinschaften, da es sich gemäß § 88 TKG um Daten handelt, die dem Fernmeldegeheimnis unterliegen.

[982] Nach § 35 Abs. 2 Nr. 3 BDSG sind die Daten zu löschen, sofern deren Speicherung nicht länger erforderlich ist. Siehe auch Schaffland/Wiltfang, BDSG, § 35 BDSG Rn. 32 mit dem Hinweis, dass diese Regelung erforderlich ist, um beim heutigen Stand der Technik und der damit verbundenen automatisierten Verarbeitung personenbezogener Daten in allen Lebenslagen, ein unbefangenes Handeln zu ermöglichen.

[983] Ein Nutzen der gespeicherten Daten gemäß § 3 Abs. 5 BDSG liegt dann vor, wenn die Daten mit einer bestimmten Zweckbestimmung ausgewertet, zusammengestellt, abgerufen oder auch nur ansonsten zielgerichtet zur Kenntnis genommen werden sollen; siehe auch Gola/Schomerus, BDSG, § 3 BDSG Rn. 42, die auf den Auffangcharakter der Regelung verweisen.

3. VPN-Kommunikation

Als weitere Dienstleistung in einem VPN kommt die Bereitstellung der VPN-Kommunikation in Betracht.[984] Hierzu ist wichtig, sich nochmals die unterschiedlichen VPN-Varianten in Erinnerung zu rufen:[985]

- Komplettmanagement des Gateways durch den Provider,
- Komplettmanagement des Gateways durch den VPN-Auftraggeber,
- Splitmanagement des Gateways, wobei für die rechtliche Bewertung hierbei entscheidend ist, in wessen Machtbereich sich der Gateway befindet. Befindet sich der Gateway im Machtbereich des VPN-Auftraggebers und übernimmt der Provider nur Wartungsaufgaben, so wurde dies als „Servicemanagement durch den Provider" bezeichnet[986]
- Software-VPN. Bei einem Software-VPN befindet sich regelmäßig in der Firmenzentrale des VPN-Auftraggebers ein Server, auf welchem die Benutzerauthentifizierung enthalten ist.[987]

In Abhängigkeit dieser verschiedenen VPN-Varianten ist geprüft worden, inwieweit der Provider im Verhältnis zu seinem Kunden (dem VPN-Auftraggeber) die Funktionsherrschaft über die Telekommunikationsanlagen des VPN innehat und damit Diensteanbieter eines eigenständigen Telekommunikationsdienstes gemäß § 3 Nr. 24 TKG ist.[988]
Im Folgenden bezieht sich die Untersuchung dementsprechend darauf, welche datenschutzrechtlichen Pflichten mit der Ausübung der Funktionsherrschaft verbunden sind.

---

[984] Siehe S. 147.
[985] Siehe S. 49 ff.
[986] Siehe S. 51.
[987] Siehe S. 53.
[988] Siehe S. 147 ff.

a. Funktionsherrschaft des VPN-Auftraggebers

Der VPN-Auftraggeber hat die Funktionsherrschaft über die VPN-Systeme inne, sofern sich der Gateway oder Server des Software-VPN im Machtbereich bzw. räumlichen Einflussbereich des VPN-Auftraggebers befindet.[989] Dies gilt sowohl beim Komplettmanagement des Gateways durch den VPN-Auftraggeber als auch beim Splitmanagement, sofern sich der Gateway im Machtbereich des VPN-Auftraggebers befindet (Servicemanagement).[990] Der Gateway oder der Server des Software-VPN sind vollständig in den Netzbetrieb seines Unternehmens eingegliedert.[991]
Der VPN-Auftraggeber, der hier im Verhältnis zum Provider die Funktionsherrschaft über den Gateway innehat,[992] wäre also unter Umständen der Verpflichtete im Sinne von § 109 Abs. 1 TKG und müsste angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses zu treffen, wozu die entsprechende Aufklärung der Mitarbeiter über die Wahrung des Fernmeldegeheimnisses gehört.[993]
Die Regelungen des § 109 Abs. 1 und Abs. 2 TKG verpflichten Diensteanbieter im Sinne des § 3 Nr. 6 TKG Vorkehrungen zum Schutze personenbezogener Daten, zum Schutz des Fernmeldegeheimnisses sowie zum Schutz der Datenverarbeitungssysteme zu treffen.[994] In Abs. 1 sind grundlegende Pflichten geregelt, die von jedem Diensteanbieter zu beachten sind, während ergänzende Pflichten in Abs. 2 geregelt werden.[995] In dieser Arbeit wird zudem § 109 Abs. 1 TKG die Verpflichtung des Diensteanbieters entnommen, seine Kunden über die Netzsicherheit zu unterrichten und diesen entsprechende Schutzmaßnahmen zu unterbreiten.[996]

[989] Siehe die Ausführungen zur Funktionsherrschaft auf S. 149 sowie Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 31.
[990] Siehe hierzu die Bildbeispiele S. 50 und S. 51.
[991] Vgl. hierzu oben S. 44 ff. sowie S. 147 ff.
[992] Vgl. oben S. 152 ff.
[993] Vgl. Gola/Klug, Grundzüge des Datenschutzrechts, S. 199; zur Einholung einer Verpflichtungserklärung (Verpflichtung auf das Datenschutzgeheimnis nach § 5 BDSG) siehe Königshofen, RDV 1997, 97, 99. Vgl. ebenso Rieß in: Bartsch/Lutterbeck, Neues Recht für neue Medien, S. 282, der darauf hinweist, dass alle Telekommunikationsdiensteanbieter ihre Mitarbeiter auf das Fernmeldegeheimnis verpflichten müssen.
[994] Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 24.
[995] Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 17.
[996] Siehe zur Informationspflicht nach § 109 Abs. 1 TKG die Ausführungen auf S. 110 ff.

Ob und wieweit solche Verpflichtungen bestehen, zeigt sich erst im Verhältnis zwischen VPN-Auftraggeber und Nutzer, was an späterer Stelle noch untersucht werden soll.[997] Auch hier ist also erforderlich, sämtliche Beteiligtenverhältnisse bei der Bereitstellung eines Online-Dienstes zu berücksichtigen. Denn nur wenn das Verhältnis zwischen VPN-Auftraggeber und Nutzer berücksichtigt wird, kann entschieden werden, inwieweit der VPN-Auftraggeber Maßnahmen im Sinne des § 109 TKG wahrnehmen muss. Im Verhältnis zum Provider steht lediglich fest, dass dem Provider gegenüber dem VPN-Auftraggeber keine datenschutzrechtlichen Verpflichtungen obliegen. Der Schutzbedarf[998] und die Anforderungen an das System müssen dementsprechend in einem anderen Personenverhältnis („VPN-Auftraggeber und Nutzer") ermittelt werden. In diesem Zusammenhang ist somit ebenso die finanzielle Leistungskraft des VPN-Auftraggebers und nicht die des Providers zugrunde zu legen. So müssen die Betreiber von Telekommunikationssystemen bzw. Telekommunikationsanlagen Maßnahmen treffen, welche unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.[999]

Die Bedeutung des Mehrpersonenverhältnisses gilt ebenso bezüglich der auf dem Gateway oder Server stattfindenden Datenverarbeitung, die erst im Verhältnis zum Betroffenen relevant wird.[1000] Bei den drei vorgenannten VPN-Varianten („Komplettmanagement des Gateways durch den VPN-Auftraggeber", „Servicemanagement im Machtbereich des VPN-Auftraggebers" und „Software-VPN") führt nicht die Tatsache der Funktionsherrschaft, sondern (erst) die inhaltliche Beschreibung und Wahrnehmung der tatsächlichen Aufgaben dazu, dass der VPN-Auftraggeber selbständig für den Datenschutz verantwortlich ist. Denn der Provider nimmt hier ausschließlich Wartungs- bzw. Serviceaufgaben wahr und hat im rechtlichen Sinne keinen Einfluss auf die auf dem Gateway oder Server stattfindende Datenverarbeitung. Der Provider ist aber kein

[997] Siehe S. 345 ff.
[998] Siehe zum Schutzbedarf Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 22.
[999] Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 21.
[1000] Vgl. zu den datenschutzrechtlichen Pflichten des VPN-Auftraggebers, Nutzers und Providers gegenüber einem Betroffenen insbesondere die Ausführungen auf S. 393 ff., 448 ff., 449 ff.

Auftragsdatenverarbeiter im Sinne von § 11 BDSG, da er personenbezogene Daten, die „auf“ einem Gateway anfallen können, nicht zielgerichtet verarbeitet oder anderweitig nutzt, sondern diese Daten bei Ausübung seiner (Service)Tätigkeit zwangsläufig anfallen.[1001]
Daher sind gemäß § 11 Abs. 5 BDSG die Regelungen von § 11 Abs. 1 bis 4 BDSG nur entsprechend anzuwenden. Deutlich wird aber, dass aufgrund der vergleichbaren Lage zu einem Auftragsdatenverarbeiter auch keine eigenständigen Löschungspflichten seitens des Providers im Hinblick auf etwaige personenbezogene Daten der Nutzer anfallen können, da nach § 11 Abs. BDSG stets der VPN-Auftraggeber für die Einhaltung der datenschutzrechtlichen Regelungen verantwortlich ist.[1002] Etwas anderes gilt nur dann, wenn der VPN-Auftraggeber den Provider zur Löschung der Daten vertraglich verpflichtet.

Das Personenverhältnis „Provider und VPN-Auftraggeber“ ist aber in diesem Zusammenhang insofern betroffen, dass der Provider dem VPN-Auftraggeber ein technisches System (VPN-System) bereitstellen muss. Ob den Provider diesbezüglich gesetzliche Pflichten, insbesondere Informations- und Aufklärungspflichten treffen können, wird im folgenden Punkt untersucht.

[1001] Gola/Schomerus, BDSG, § 11 BDSG Rn. 14 nehmen Bezug auf Wartungs- und Serviceunternehmen, die personenbezogene Daten bei Ausübung ihrer Tätigkeit „beiläufig“ zur Kenntnis nehmen müssen. Gegenstand von Wartung oder Service ist nicht dem ausführenden Unternehmen Kenntnis über personenbezogene Daten zu verschaffen, sondern die Leistung besteht hauptsächlich darin, die (Datenverarbeitungs-)Systeme instand zu halten. Dennoch ist der Schutz der Daten geboten, da eine Kenntnisnahme durch den Provider bzw. Service-Unternehmer grundsätzlich möglich ist.
[1002] Siehe auch Gola/Schomerus, BDSG, § 11 BDSG Rn. 3 mit dem Hinweis, dass die Auftraggeberin „Herrin der Daten“ ist und bleibt. Schneider, Handbuch des EDV-Rechts, Teil B Rn. 218 verweist ebenso darauf, dass § 11 BDSG die Rechte des Betroffenen nicht verkürzen soll und der Auftraggeber Herr der Daten bleibt, damit im Verhältnis zum Betroffenen datenschutzrechtlich verantwortlich ist. Der Auftragnehmer ist hierbei nicht Dritter (Schneider, Handbuch des EDV-Rechts, Teil B Rn. 197).

aa. Technische Schutzmaßnahmen

Die Frage, inwieweit der Provider dennoch zur Information und Aufklärung über die Netzsicherheit gemäß § 109 Abs. 1 TKG verpflichtet ist,[1003] auch wenn der VPN-Auftraggeber die Funktionsherrschaft über die VPN-Systeme innehat, stellt sich bei den folgenden VPN-Varianten:

- „Software-VPN“
- „Komplettmanagement durch den VPN-Auftraggeber“
- und „Splitmanagement im Machtbereich des VPN-Auftraggebers“ (Servicemanagement durch den Provider)

Zu berücksichtigen ist bei diesen Varianten, dass der Provider lediglich die Funktionsherrschaft über den Internetzugangsknoten und nicht über den Gateway bzw. beim Software-VPN nicht über den Server innehat.[1004]
So verpflichtet aber Artikel 4 Abs. 2 der EU-Richtlinie 2002/58/EG, dessen Intention auch in § 109 TKG bzw. in dem Erfordernis der „angemessenen“ Schutzmaßnahmen Berücksichtigung gefunden hat,[1005] den Provider, den Nutzer und Teilnehmer über mögliche Abhilfen (dennoch) zu unterrichten, (auch) wenn das Risiko außerhalb des Anwendungsbereichs der von dem Provider zu treffenden Maßnahmen liegt.
Hierbei besteht eine Überschneidung zu den Pflichten gemäß § 93 TKG, da hier ebenfalls eine Unterrichtung über die Verwendung[1006] von personenbezogenen Daten sowie die grundlegenden Verarbeitungstatbestände normiert ist.

Bietet ein Provider ein Komplettpaket VPN in dem Sinne an, dass er dem VPN-Auftraggeber „nur“ die Internetzugänge und ebenso die entsprechende VPN-Technik zur Verfügung stellt, dann sind ihm die Pläne des VPN-Auftraggebers zumindest bekannt. Dies gilt gleichermaßen, wenn der VPN-Auftraggeber letztendlich selbst für das Management des VPN verantwortlich ist oder der Provider ausschließlich Wartungsarbeiten übernimmt.

[1003] Siehe zur Informationspflicht nach § 109 Abs. 1 TKG die Ausführungen auf S. 110 ff.
[1004] Siehe hierzu die Ausführungen mit Bildbeispielen auf S. 53 ff. (Software-VPN) und S. 50 (Systemmanagement des Kunden).
[1005] Siehe hierzu die Ausführungen auf S. 110 ff.
[1006] Siehe zum Oberbegriff „Verwendung“ für die Verarbeitung und Nutzung von Daten Gola/Schomerus, BDSG, § 3 BDSG Rn. 25.

Daher kann hier unter Berücksichtung des Artikels 4 Abs. 2 der EU-Richtlinie 2002/58/EG die berechtigte Frage gestellt werden, ob dem Provider dennoch Informationspflichten über technische „Abhilfen“ obliegen, auch wenn das Risiko außerhalb des Anwendungsbereichs der von dem Provider zu treffenden Maßnahmen liegt.

Dafür spricht, dass seitens des VPN-Auftraggebers erheblicher Aufklärungsbedarf besteht und der Provider einen technischen Wissensvorsprung hat. Der Provider kann einschätzen, welche Techniken für die Zwecke des einen VPN-Auftraggebers gut geeignet sein können, für die Zwecke eines anderen VPN-Auftraggebers aber gegebenenfalls nicht brauchbar sind. Dies zeigt sich im Besonderen bereits bei der Entscheidung, ob ein Software-VPN oder ein Gateway-VPN eingerichtet werden soll. So wird bei Software-VPN-Produkten[1007] ebenso IPSec[1008] angeboten, obwohl hierzu vertreten wird, dass dieses Protokoll grundsätzlich selten unmittelbar zwischen zwei Clients bzw. Rechnern im Internet eingesetzt wird.[1009] Daher besteht Aufklärungsbedarf, inwieweit die Sicherheit der Daten bei einer reinen Software-Lösung, also einem Software-VPN und Verbindung von Rechner zu Rechner, beeinträchtigt wird.

Fragen zur Sicherheit tauchen ebenso dahingehend auf, inwieweit die Verwaltung der Passwörter durch den Administrator[1010] bzw. die Verwaltung des VPN-Betriebs auf einem Rechner des Kunden zu Sicherheitslücken führen kann, und inwieweit dies durch die Verwendung eines gesonderten Gateway vermieden werden kann. Ebenso gibt es bei Gateway-VPN technische Unterschiede.[1011] So gibt es beispielsweise die Möglichkeit der Zertifizierung von Gateways. Insbesondere sind Gateways, die die Schnittstelle zwischen einem Intranet und dem Internet darstellen, in besonderem Maße gegen

[1007] Siehe das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch“, S. 3.
[1008] Siehe zu IPSec S. 39 ff.
[1009] Siehe Lipp, VPN; S. 205.
[1010] Vgl. das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch“, S. 18.
[1011] So gibt es etwa die separate Möglichkeit, gewisse Zertifizierungen in Anspruch zu nehmen. Vgl. hierzu etwa das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 20 ff.

Zugriffe zu schützen sind, [1012] wobei vertreten wird, dass aus diesem Grunde der Einsatz von Routern vermieden werden sollte.[1013]
Wünschenswert ist daher, wenn der VPN-Auftraggeber umfassend darüber aufgeklärt werden würde, inwieweit die verschiedenen Techniken Auswirkungen auf die Datensicherheit und Datenvermeidung haben.[1014] Nichtsdestotrotz erscheint es in den Fällen, in welchen der VPN-Auftraggeber die Funktionsherrschaft über das System ausübt, als nicht gerechtfertigt, den Provider insgesamt den strengen Verpflichtungen der § 109 Abs. 1 TKG unter Berücksichtigung des Artikels 4 und des Erwägungsgrundes 20 der EU-Richtlinie 2002/58/EG zu unterwerfen. Ebenso wenig sollten ihm gesetzliche Unterrichtungspflichten gemäß § 93 TKG obliegen. Denn zu berücksichtigen ist in diesen Fallgestaltungen, dass der Provider lediglich den Internetzugang bereit stellt und ansonsten „nur" Anbieter einer Software-Lösung oder Auftragsdatenverarbeitung gemäß § 11 Abs. 5 BDSG ist. Insoweit besteht also kein Unterschied zu anderen VPN-Anbietern, die allein Hardware und/oder Software –ohne Internetzugang- anbieten.[1015] Diese Software- und Hardwareanbieter werden durch die Bereitstellung der VPN- Techniken ebenso wenig zum Diensteanbieter gemäß § 3 Nr. 6 TKG, so dass eine nicht zu rechtfertigende Ungleichbehandlung vorliegen würde, sofern die staatliche Regulierungsbefugnis für den Provider des Komplettpaketes VPN greifen würde.

Sofern also im Sinne der dienstorientierten[1016] Betrachtungsweise die einzelnen Dienste getrennt voneinander zu betrachten sind, muss dies gleichermaßen für die damit verbundenen Rechtsfolgen gelten.

[1012] Vgl. auch Lipp, VPN, S. 58, der darstellt, dass ein Gateway in sicheren Umgebungen betrieben werden sollten und nicht in normalen Büroräumen. Außerdem sollten Gateways spezielle Mechanismen zum Schutz gegen verschiedene Arten von Angriffen aufweisen, und zwar auch gegenüber Mitarbeitern.
[1013] Siehe Lipp, VPN, S. 346; Campo/Pohlmann, Virtual Private Networks, S.130/300, die auf die Schwächen von Routern bei einer VPN-Realisierung verweisen. Siehe ebenso Fn. 204 in dieser Arbeit.
[1014] Zur Datenvermeidung siehe die Ausführungen auf S. 106 ff. Vgl. außerdem die Ausführungen auf S. 218 Fn. 938 mit Verweis auf die Möglichkeit des „Umsteigebahnhofs".
[1015] Vgl. hierzu in der Einführung die Ausführungen auf S. 4, insbesondere Fn. 18. Eine andere Frage ist, inwieweit sich in zivilrechtlicher Hinsicht vertragliche Aufklärungspflichten über die unterschiedlichen Sicherheitsrisiken ergeben könnten. Diese Frage soll in dieser Arbeit jedoch nicht behandelt werden.
[1016] Vgl. hierzu oben S. 74/86.

Die Intention von Artikel 4 Abs. 2 der EU-Richtlinie 2002/58/EG sowie die angemessenen Schutzvorkehrungen zum Schutze des Fernmeldegeheimnisses und der personenbezogenen Daten gemäß § 109 Abs. 1 TKG sind erfüllt, wenn der Provider im Sinne seiner Funktion als Access-Provider über gängige Verschlüsselungstechniken wie SSL aufklärt.[1017]

Insgesamt ist festzustellen, dass dem (Access-)Provider keine Aufklärungspflicht bezüglich der unterschiedlichen VPN-Techniken obliegen kann, sofern der VPN-Auftraggeber die Funktionsherrschaft über das System bzw. die Telekommunikationsanlage ausübt. Dies gilt auch dann, wenn er solche VPN-Techniken zusätzlich anbietet.
Der im zweiten Abschnitt dieser Arbeit enthaltene Überblick bezüglich der unterschiedlichen VPN-Techniken,[1018] lässt zwar bereits die Schwierigkeit und Vielschichtigkeit eines VPN erkennen. Er zeigt gleichermaßen, dass aufgrund der umfassenden und schwierigen technischen Details eines VPN grundsätzlicher Aufklärungsbedarf und Informationsbedarf besteht. Dabei ist es aber stets von besonderer Bedeutung, inwieweit einem kommerziellen Anbieter gesetzliche Unterrichtungspflichten und angemessene technische Schutzvorkehrungen gemäß §§ 93, 109 TKG obliegen.
Bei anderer Bewertung wäre letztendlich jeder Access-Provider zur Aufklärung über VPN-Protokolle verpflichtet, da hier ebenfalls argumentiert werden könnte, dass dies Maßnahmen außerhalb seines Verantwortungsbereiches sind, über die er aber dennoch aufklären muss.
Dies bedeutet, dass der Provider in diesen Fällen im Verhältnis zum VPN-Auftraggeber lediglich Diensteanbieter bezüglich der Bereitstellung des Internetzugangs ist und damit den gleichen Verpflichtungen unterliegt wie im Verhältnis zu anderen Kunden, denen er ebenfalls einen Internetzugang bereit stellt. Ihm obliegen daher gemäß TKG keine Unterrichtungspflichten oder die Sicherstellung von angemessenen Schutzmaßnahmen. Es wäre in diesem Falle darüber hinaus zu untersuchen, ob dem Provider aus zivilrechtlichen Gesichtspunkten Aufklärungspflichten obliegen könnten. Dies soll in dieser datenschutzrechtlichen Arbeit jedoch nicht (ergänzend) betrachtet werden und daher lediglich darauf verwiesen werden, dass als Gegenstand der

[1017] Vgl. hierzu oben S. 196 ff.
[1018] Siehe hierzu die Ausführungen mit Bildbeispielen auf S. 44 ff.

Aufklärungspflicht solche Umstände in Betracht kommen, die geeignet sind, den Vertragszweck des anderen zu vereiteln oder jedenfalls für die Entschließung des anderen Teils von Bedeutung sind.[1019] Hierbei sind auch ein mögliches Informationsgefälle und das besondere Schutzbedürfnis des anderen Teils zu beachten, sofern er keine Möglichkeit hatte, sich hinreichend zu informieren oder sachkundige Fragen zu stellen.[1020]

bb. Auskunfts- und Überwachungsmaßnahmen

Sofern sich der Gateway oder der Server des Software-VPN im Machtbereich des VPN-Auftraggebers befinden und dieser die Funktionsherrschaft innehat, obliegen dem Provider im Hinblick auf die Daten, die mittels bzw. auf dem Gateway verarbeitet werden, keine gesetzlichen Auskunftsansprüche gemäß § 113 TKG[1021] oder Überwachungsmaßnahmen im Sinne der TKÜV.[1022] Da das Management eines Gateway nicht durch den Provider erfolgt, und er in diesem Zusammenhang ebenso wenig Anbieter eines Telekommunikationsdienstes gemäß § 3 Nr. 6 TKG ist, können sich die gesetzlichen Auskunftspflichten allein auf die von ihm erbrachte Dienstleistung der Bereitstellung des Internetzugangs beziehen. Diesbezüglich wurde bereits dargestellt, dass es sich bei der Bereitstellung eines Internetzugangs um einen Telekommunikationsdienst im Sinne von § 3 Nr. 24 TKG.[1023] Bei einem Internetzugangsknoten, wie beispielsweise dem PoP, handelt es sich darüber hinaus um eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG.[1024]

An dem Internetzugangsknoten kommt die Kommunikation allerdings bereits verschlüsselt an, da der Rechner und der Gateway die entscheidenden Stellen zur Verschlüsselung sind.[1025] Der Access-Provider wäre daher nur verpflichtet, den gemäß § 113 TKG oder § 2 Nr. 2 TKÜV berechtigten Stellen

[1019] Struck, MMR 2001 507, 510.
[1020] Struck, MMR 2001 507, 510.
[1021] Siehe zu dessen Voraussetzungen S. 200.
[1022] Zur TKÜV siehe S. 12, insbesondere Fn. 46.
[1023] Siehe S. 122 ff. Zum Begriff der Telekommunikation als Austausch von Informationen durch Transport über gewisse Entfernungen siehe Schuster in: TKG-Kommentar (2. Auflage), § 3 TKG Rn. 19; ebenso Piepenbrock/Attendorn/Schuster/Wittern in: TKG-Kommentar (3. Auflage), § 3 TKG Rn. 45.
[1024] Siehe S. 114. Siehe auch Wuermeling/Felixberger, CR 1997, 230, 233.
[1025] Siehe oben S. 44 ff.

(beispielsweise Strafverfolgungsbehörden) die verschlüsselte Kommunikation herauszugeben.[1026] Eine Verpflichtung des Providers dahingehend, den Datenschlüssel herauszugeben bzw. die Verschlüsselung aufzuheben, kann hingegen nicht verlangt werden. Die Kenntnis bezüglich der Sicherheitsstrategie des VPN-Auftraggebers erhält der Provider aufgrund einer anderen Funktion. Denn zu betonen ist in diesem Zusammenhang folgendes: Selbst wenn der Provider durch das Splitmanagement bzw. Servicemanagement Einblick in die Daten und Kenntnis über die Sicherheitsstrategie des sich *in den Räumen des VPN-Auftraggebers* befindlichen Gateway erhalten würde, würde er dieses Wissen um den generierten Datenschlüssel[1027] oder der verschlüsselten Daten nicht in seiner Eigenschaft als Anbieter eines Telekommunikationsdienstes, sondern als Auftragsdatenverarbeiter[1028] gemäß § 11 Abs. 1, Abs. 5 BDSG bzw. als „reiner" Auftragnehmer erhalten würde. Denn sofern keine personenbezogenen Daten Dritter verarbeitet werden, sondern „nur die eigenen" Daten des VPN-Auftraggebers, dann kommt keine Auftragsdatenverarbeitung gemäß § 11 BDSG in Betracht, aber der Provider handelt in diesem Falle dennoch als Auftragnehmer, dessen Auftrag sich auf das Management des Gateways und die Verarbeitung der Daten des Auftragnehmers bezieht.[1029] So übernähme der Provider bezüglich des Systemmanagements keine andere Funktion als ein sonstiger Dienstleister, der für das VPN die Hard- oder Software bereitstellt oder mit der Sicherheitsstrategie des VPN betraut ist.

[1026] Vgl. zur Hinterlegungspflicht von verwendeten Schlüsseln Schaar in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 402, der dies ablehnt. Vgl. ebenso Baum/Trafkowski, CR 2002, 69, 70, die sich insgesamt gegen eine gesetzliche Einschränkung der Verwendung von Verschlüsselungsprodukten aussprechen und in diesem Zusammenhang einen französischen Gesetzesentwurf vorstellen, der eine Strafrahmenerhöhung vorsieht, soweit bei der Vorbereitung oder Begehung einer Straftat Verschlüsselungsmethoden eingesetzt wurden. Siehe außerdem Hamm in: Holznagel/Nelles/Sokol, TKÜV, S. 88, der ausführt, dass gemäß § 8 Abs. 2 TKÜV die von Betreibern eingesetzten Schutzverfahren den Schlüssel auszuliefern haben, dass aber noch nicht vorgesehen ist, dass auch die Nutzer die von ihnen selbst eingesetzten Kryptoprogramme mitliefern oder die Verschlüsselung zu unterlassen haben.
[1027] Siehe zur Verschlüsselung S. 41 ff.
[1028] Siehe ebenso die Ausführungen bei Gola/Schomerus, BDSG, § 11 BDSG Rn. 14 sowie S. 231 ff. in dieser Arbeit.
[1029] Siehe zu § 28 Abs. 1 BDSG und zum „eigenen Geschäftszweck" S. 208.

Entscheidend ist, dass allein durch die Bereitstellung von Software oder Servicediensten der Provider nicht zu einem Telekommunikationsdiensteanbieter gemäß § 3 Nr. 6 TKG wird.[1030]
Allerdings sind nur Telekommunikationsdiensteanbieter gemäß § 113 Abs. 1 TKG zur Auskunft oder gemäß § 3 Abs. 1 TKÜV zur Überwachung und Aufzeichnung der Telekommunikation verpflichtet.
Auch § 8 Abs. 3 TKÜV regelt eindeutig, dass nur derjenige, der die ihm zur Übermittlung anvertraute Telekommunikation *netzseitig* durch technische Maßnahmen gegen die unbefugte Kenntnisnahme durch Dritte schützt, die Kenntnisnahme der ungeschützten Telekommunikation ermöglichen muss.
Für einen „reinen“ Access-Provider wäre es im Übrigen gar nicht möglich, Verschlüsselungen mit hohem Sicherheitsstandard, wie von IPSec geboten, aufzuheben oder den Strafverfolgungsbehörden entsprechende Möglichkeiten zur Aufhebung bereit zu stellen.

Als Fazit gilt, dass die unterschiedlichen Techniken eines VPN genau zu untersuchen und streng nach ihren Funktionen und Möglichkeiten zu trennen sind, da dies im Hinblick auf die rechtliche Bewertung erhebliche Auswirkung hat.

b. Funktionsherrschaft des Providers

Sofern der Provider das Komplettmanagement des VPN bzw. des Gateway des VPN übernimmt, hat er auch die Funktionsherrschaft inne.[1031]
Gleiches gilt beim Spitmanagement, sofern sich der Gateway zwar im Machtbereich des Providers befindet, aber das Management des Gateway zwischen VPN-Auftraggeber und Provider derart aufgeteilt ist, dass der Provider lediglich Wartungsaufgaben übernimmt und der VPN-Auftraggeber durch entsprechende administratorische Fernzugriffsrechte die Sicherheitsstrategie des Gateway selbst bestimmen darf.[1032]

[1030] Vgl. auch Pernice, DuD 2002, 207, 209, die darstellt, dass der Betreiber ***netzseitige*** Verschlüsselungen, die er als Dienstleistung Dritten anbietet, selbst aufheben bzw. der berechtigten Stelle ermöglichen muss, diese für die abzuhörenden Daten aufzuheben.
[1031] Siehe S. 154 ff.
[1032] Siehe hierzu die Darstellung auf S. 52 sowie die rechtlichen Ausführungen auf S. 156

Vor diesem Hintergrund wird die Frage bedeutsam, inwieweit dem Provider gegenüber dem VPN-Auftraggeber datenschutzrechtliche Pflichten obliegen. Um diese Frage beantworten zu können, basiert die datenschutzrechtliche Prüfung wiederum auf dem bereits im zweiten Abschnitt vorgestellten Prüfungsschema. Es werden wiederum die Themen „Datenvermeidung", „Bereitstellung der technischen Sicherheitsmaßnahmen" sowie „Verpflichtung zur Übernahme gesetzlicher Auskunfts- und Überwachungspflichten" behandelt.[1033]

aa. Datenvermeidung bei Protokolldaten

Auf dem Gateway werden regelmäßig die einzelnen Zugriffe registriert und entsprechende Protokolle bzw. Log-Files erstellt.[1034]
Diejenigen, die zur weiteren Erbringung des Telekommunikationsdienstes nicht benötigt werden, sind gemäß § 96 Abs. 2 TKG unverzüglich zu löschen.
In diesem Rahmen ist zu berücksichtigen, inwieweit eine Speicherung zu den in §§ 97 ff. TKG genannten Zwecken in Betracht kommen kann. So ist insbesondere die Aufbewahrung der Log-Files für Zwecke der Vermeidung und Behebung von technischen Störungen (§ 100 Abs. 1 TKG) erforderlich.

Hier stellt sich gleichermaßen die Frage nach der Dauer von Aufbewahrungsfristen. Entsprechend der Ausführungen zum Access-Providing sollten keine Mindestspeicherungsfristen normiert werden.[1035] Der Verzicht auf solche Fristen wäre dann nicht problematisch, sofern die Provider in einem nachvollziehbaren Datenschutzkonzept darlegen, aus welchen Gründen eine Datenspeicherung im Einzelfall für eine bestimmte Dauer unbedingt erforderlich ist.[1036] Es könnten hierbei gewisse Erfahrungswerte zugrunde gelegt werden, beispielsweise dass zur Behebung von Störungen regelmäßig eine Dauer von

[1033] Siehe S. 106 ff.
[1034] Siehe zu Log-Files ebenso S. 178.
[1035] Siehe S. 175 ff.
[1036] Vgl. hierzu die Ausführungen zum Access-Providing auf S. 170 ff. sowie Ohlenburg, MMR 2004, 431, 437, die ebenso gegen die Vorgabe von konkreten Löschungspflichten argumentiert. Siehe zu den Vorgaben einer Speicherdauer und einer am Einzelfall orientierten Betrachtungsweise auch Schoen, DuD 2005, 84, 86 (der sich in seinen Ausführungen allerdings auf die gesetzliche Grundlage des TDDSG bezieht).

zwei Wochen ausreichend ist. [1037]
Ein solches Datenschutzkonzept könnte jederzeit durch eine Datenschutzaufsichtsbehörde überprüft werden. Gelingt es dem Provider nicht, Speicherungsfristen nachvollziehbar darzulegen, so kann die Behörde gemäß § 115 TKG für entsprechende Abhilfe sorgen, die letztendlich ebenso die Einstellung des Dienstes umfasst (§ 115 Abs. 3 TKG). Insbesondere die oben zitierte Entscheidung des LG Darmstadt zeigt,[1038] dass es für ein Gericht ohne Einschaltung entsprechender Gutachter nahezu unmöglich ist, eine sachgerechte Entscheidung bezüglich Speicherfristen zu treffen. Befasst sich allerdings im Sinne von § 115 TKG der Bundesbeauftragte für Datenschutz mit der Frage der Zulässigkeit von Speicherungsfristen befasst, so hat dies den entscheidenden Vorteil, dass von vorneherein eine technisch versierte Behörde den Sachverhalt bewerten kann.

bb. Geheimhaltungspflichten

Eine weitere wesentliche Frage ist, inwieweit ein Provider beim Komplettmanagement eines Gateway und entsprechender Funktionsherrschaft Einfluss auf die Sicherheit des VPN hat und inwieweit er bei Durchführung des Komplettmanagement durch datenschutzgesetzliche Vorgaben gebunden ist. So interessiert vor allem, inwieweit der generierte Datenschlüssel, der für den Schutz der Daten verantwortlich ist, seitens des Providers der Geheimhaltung unterliegt. Hierzu wurde oben eingehend die Verschlüsselungstechnik dargestellt und ausgeführt, dass bei den einzelnen Datenübertragungsvorgängen jeweils Schlüssel generiert und über das Internet übertragen werden.[1039]

Im Rahmen der folgenden Untersuchung wird danach unterteilt, ob es sich bei dem VPN-Auftraggeber um eine natürliche oder juristische Person handelt, weil sich bei natürlichen Personen die entsprechenden datenschutzrechtlichen Pflichten des Providers unmittelbar aus dem BDSG ergeben könnten (was zu untersuchen ist). Da das BDSG für juristische Personen hingegen keine

[1037] Siehe S. 180 ff.
[1038] Siehe S. 173 ff.
[1039] Siehe S. 41 ff.

Anwendung findet, werden die Interessen von juristischen Personen gesondert geprüft.

aaa. Natürliche Personen

Für natürliche Personen gilt, dass es sich bei dem Schlüssel um ein personenbezogenes Datum gemäß § 3 BDSG handelt. Dies folgt daraus, dass der Schlüssel speziell für den VPN-Auftraggeber und für die Verschlüsselung von dessen Daten generiert wird und sich somit ein unmittelbarer Bezug zu diesem herstellen lässt.[1040]

Insbesondere handelt es sich bei dem erzeugten Schlüssel auch um eine Einzelangabe im Sinne des BDSG,[1041] und nicht um ein Verkehrsdatum des § 96 Abs. 1 TKG, da der Schlüssel nicht unter dessen abschließende Aufzählung subsumiert werden kann.[1042]
Zu beachten ist, dass im Verhältnis zwischen Provider und VPN-Auftraggeber das BDSG aufgrund § 1 Abs. 2 Nr. 3 BDSG „unmittelbar“ [1043] Anwendung findet. Denn der Provider ist als nicht-öffentliche Stelle mit der Verarbeitung der personenbezogenen Daten des VPN-Auftraggebers (in Form des generierten Schlüssels) beauftragt. Der Provider ist daher seinem Auftraggeber gegenüber datenschutzrechtlich verpflichtet und muss im Sinne von § 9 BDSG die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten.[1044] Die Regelung der Auftragsdatenverarbeitung gemäß § 11 BDSG findet nur insoweit Anwendung, wenn ebenso personenbezogene Daten Dritter (etwa Kunden des VPN-Auftraggebers) verschlüsselt werden. Ansonsten werden lediglich eigene personenbezogene Daten des VPN-Auftraggebers verarbeitet.

[1040] Gola/Schomerus, BDSG, § 3 BDSG Rn. 9; Schulz, Die Verwaltung 1999, 137, 163.
[1041] Vgl. zu den personenbezogenen Daten Gola/Schomerus, BDSG, § 3 BDSG Rn. 3; Schulz in: Roßnagel, Recht der Multimedia-Dienste, § 1 TDDSG Rn. 28; Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 279. Siehe außerdem zu den personenbezogenen Daten die Ausführungen auf S. 92 ff.
[1042] Vgl. zum abschließenden Charakter des § 96 Abs. 1 TKG, der § 6 Abs. 1 TDSV ersetzt hat, Büchner in: TKG-Kommentar (2. Auflage), § 5 TDSV (Anh § 89 TKG) Rn. 1; Robert in: TKG-Kommentar (3. Auflage), § 96 TKG Rn. 2.
[1043] Siehe außerdem zur zulässigen Speicherung personenbezogener kreditrelevanter Daten über Ein-Mann-GmbH-Gesellschafter BGH, NJW 1986, 2505, 2505.
[1044] § 9 BDSG kommt hier aus dem Grunde zur Anwendung, da keine vorrangigen Regelungen des TKG in Betracht kommen. Zum Exklusivitätsverhältnis zwischen BDSG und TKG siehe auch S. 92.

In diesem Zusammenhang ist ebenso zu berücksichtigen, dass bei der Verschlüsselung ein Schlüssel generiert wird, der aus Sicherheitsgründen nach jedem Übertragungsvorgang sofort gelöscht werden muss. Die Schlüssel werden nur solange benötigt, bis das letzte übertragene Paket innerhalb der Lebensdauer einer Sicherheitsassoziation vom Empfänger verschlüsselt wurde. Die erforderliche Lebensdauer liegt regelmäßig im einstelligen Sekundenbereich.[1045] Eine längere Speicherung birgt ein erhebliches Sicherheitsrisiko, da nur aufgrund eines einziges bekannt gewordenen privaten Schlüssels auf einer der beiden Seiten einer Sicherheitsassoziation, Vertraulichkeit, Integrität und Authentizität der übertragenen Pakete nicht mehr gewährleistet sind. Aus diesem Grunde muss die private Komponente des Schlüssels sofort nach Erzeugung des symmetrischen Schlüssels sicher vernichtet werden.[1046]

Der Provider muss daher gemäß § 9 BDSG dafür Sorge tragen, dass der Schlüssel geheim gehalten und zuverlässig vernichtet wird.[1047] Er muss gemäß § 5 BDSG gleichermaßen seine Mitarbeiter entsprechend verpflichten.

Die Vernichtung stellt dann eine erforderliche Maßnahme dar, wenn sie in einem angemessenen Verhältnis zum Aufwand steht, wobei sich die Schutzkriterien konkret an der Schutzbedürftigkeit der einzelnen Daten zu orientieren haben.[1048] Bereits der Einsatz eines VPN und die Verschlüsselung der Daten mittels IPSec muss allerdings für den Provider als sicheres Indiz gewertet werden, dass der VPN-Auftraggeber ein sehr hohes Schutzbedürfnis hat und der Schlüssel vernichtet werden muss.

bbb. Juristische Personen und Personengemeinschaften

Im Hinblick auf den Schutz juristischer Personen und Personengemeinschaften, auf die das BDSG keine Anwendung findet, wäre der Provider nicht von Gesetzes wegen zur Geheimhaltung und Löschung des Schlüssels verpflichtet. Eine solche Löschungsverpflichtung müsste in einer separaten, vertraglichen

[1045] Lipp, VPN, S. 226.
[1046] Lipp, VPN, S. 226.
[1047] Siehe hierzu auch Schaar, Datenschutz im Internet, Rn. 163.
[1048] Siehe Gola/Schomerus, BDSG, § 9 BDSG Rn. 7/9.

Verpflichtungserklärung zum Schutze und Umgang von Geschäfts- und Betriebsgeheimnissen berücksichtigt werden.

Der generierte Schlüssel fällt unter den Begriff des Betriebs- und Geschäftsgeheimnisses.[1049] Hierunter ist jede im Zusammenhang mit einem Geschäftsbetrieb stehende, nicht offenkundige Tatsache zu verstehen ist, an deren Geheimhaltung der Betriebsinhaber ein berechtigtes wirtschaftliches Interesse hat und die nach seinem bekundeten oder erkennbaren Willen auch geheim bleiben soll.[1050] Unter Betriebs- und Geschäftsgeheimnissen sind beispielsweise Konzepte, Know-How, nicht veröffentlichte Patentanmeldungen, Erfindungen zu verstehen. Im Allgemeinen beziehen sich Geschäftsgeheimnisse auf den kaufmännischen Geschäftsverkehr, wie etwa Kundenadressen, Geschäftsbriefe,[1051] wohingegen unter dem Begriff „Betriebsgeheimnis“ regelmäßig der technische Betriebsablauf verstanden wird.[1052] Hiervon ist alles umfasst, woran ein Unternehmer, der nicht notwendigerweise eine juristische Person sein muss, ein geheimhaltungswürdiges Interesse hat.[1053]

Vgl. außerdem zu Betriebs- und Geschäftsgeheimnissen BAG, NJW 1988, 1686; 1687 (Kundenliste und Kaufgewohnheiten als Geschäftsgeheimnisse); Schaub, Arbeitsrechts-Handbuch, § 54 Rn. 2, der darauf verweist, damit alle Tatsachen gemeint sind, die in einem Zusammenhang mit einem Geschäftsbetrieb stehen, nur einem eng begrenzten Personenkreis bekannt und nicht offenkundig sind, nach dem Willen des Arbeitgebers und im Rahmen eines berechtigten wirtschaftlichen Interesses geheim gehalten werden sollen (hierzu gehören etwa technisches Know-How, auch wenn es nicht patentfähig ist, Bilanzen, Erfindungen von Arbeitnehmern, etc.). Ebenso Kunz, DB 1993, 2482, 2483, der anmerkt, dass die Grenzen zwischen Geschäftsgeheimnissen und Betriebsgeheimnissen fließend und daher entscheidend sei, dass es sich bei der Tatsache um ein Geheimnis handelt. Siehe auch Molkenbur, BB 1990, 1196, 1197, der zur Patentanmeldung anmerkt, dass nur bis zur deren Offenlegung der Anmelder verlangen könnte, dass sein bis dahin ungeschütztes Recht nicht durch vorzeitige Preisgabe verwertet wird. Siehe zur Verschwiegenheitspflicht im Arbeitsrecht bezüglich Geschäfts- und Betriebsgeheimnissen die Ausführungen von Taeger, Arbeit und Arbeitsrecht 1992, 201 ff., der feststellt, dass es einen absoluten Geheimnisschutz nicht geben kann (aaO S. 203).

[1050] Köhler in: Köhler/Piper UWG-Kommentar, § 17 Rn. 4; BGH, GRUR 1955, 424, 425; Hefermehl/Köhler/Bornkamm, UWG-Kommentar, § 17 Rn. 4; siehe auch Wiebe, Know-how-Schutz von Computersoftware, S. 221, mit der Anmerkung, dass nach überwiegender Meinung Geheimhaltungswille und -interesse gemeinsam vorliegen müssen. Es ist erforderlich, dass der Betriebsinhaber den Willen zur Geheimhaltung sowie ein berechtigtes wirtschaftliches Interesse an der Geheimhaltung einer nicht offenkundigen Tatsache hat (Köhler in: Köhler/Piper, UWG-Kommentar, § 17 Rn. 6-8; Tinnefeld, DUD 2002, 231, 236), wobei das Geheimnis nicht notwendigerweise einen Vermögenswert darstellen muss, sondern ausreichend ist, dass sich die Kenntnis Dritter für das Unternehmen nachteilig auswirken kann (Köhler in: Köhler/Piper, UWG-Kommentar, § 17 Rn. 9).

[1051] BGH, WRP 1999, 912, 914; OLG Hamm, WRP 1993, 118, 119; Köhler in: Köhler/Piper, UWG-Kommentar, § 17 Rn. 4.

[1052] BAG, NJW 1988, 1686, 1686; Köhler in: Köhler/Piper, UWG-Kommentar, § 17 Rn. 4.

[1053] Vgl. auch Wiebe, Know-how-Schutz von Computersoftware, S. 220 ff., wonach ein berechtigtes Interesse an der Geheimhaltung unter anderem vorliegen kann, wenn ihm diese Geheimhaltung einen Wettbewerbsvorsprung, Verbesserung der Wettbewerbsstellung,

In rechtspolitischer Hinsicht ist ergänzend die Frage zu stellen, ob sich durch die mangelnde Gleichstellung zwischen personenbezogenen Daten und Geschäfts- und Betriebsgeheimnissen im Hinblick auf strafbares Verhalten des Providers ein Unterschied ergeben könnte.[1054]
Handelt es sich beim VPN-Auftraggeber um eine natürliche Person, macht sich der Provider gemäß §§ 43, 44 BDSG strafbar, sofern er den Datenschlüssel an einen Dritten weitergibt oder offenbart. Dies ergibt sich daraus, dass nach §§ 43 Abs. 2 Nr. 1, 44 BDSG das unbefugte Verarbeiten von Daten eine Ordnungswidrigkeit darstellt bzw. strafbar ist. Die Rechtswidrigkeit ergibt sich hierbei aus den Erlaubnistatbeständen des BDSG für die Verarbeitung, wie beispielweise § 4 Abs. 1 BDSG oder §§ 28 ff. BDSG.[1055] Sofern der Provider das Komplettmanagement des Gateways übernimmt und damit auch für Sicherheit und Datenverschlüsselung Sorge trägt, dann generiert er den Datenschlüssel für eigene Geschäftszwecke, nämlich um den mit dem VPN-Auftraggeber eingegangenen VPN-Managementvertrag zu erfüllen.[1056]
Dementsprechend kommt eine Strafbarkeit im Sinne des § 43 Abs. 2 Nr. 1, § 44 Abs. 1 BDSG in Verbindung mit § 3 Abs. 4 Nr. 3 BDSG in Betracht, sofern der Provider den generierten Datenschlüssel (einer natürlichen Person) an einen Dritten ohne Einwilligung des VPN-Auftraggebers übermittelt.[1057]

Verbesserung der Markteintrittschancen oder sonstigen Vorteil vor Konkurrenten gewährt, und das Bekanntwerden geeignet ist, den Wettbewerb des Konkurrenten zu steigern oder sonst den Betrieb zu schädigen. Dabei hat auch das Erfordernis der Nichtoffenkundigkeit zentrale Bedeutung (S. 221). Es kann sich aber auch um Strategien der Geschäftsführung, Unternehmensplanung oder Personalführung handeln, ohne dass hier unmittelbar ein Vorteil vor Konkurrenten im Vordergrund steht(vgl. Wiebe, Know-how-Schutz von Computersoftware, S. 221, der darauf hinweist, dass ebenso allein die Tatsache, dass ein bestimmtes Verfahren in einem Betrieb verwendet wird, als Geheimnis schutzfähig sein kann). Siehe auch die beispielhafte Übersicht bei Harte-Bavendamm/Henning-Bodewig, UWG-Kommentar, § 17 UWG Rn. 7.

[1054] Vgl. auch das im Frühjahr 2001 für den Bundesminister des Inneren erstattete Gutachten „Modernisierung des Datenschutzrechts“, S. 65, von Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001, im Folgenden: Modernisierungsgutachten. Siehe ebenso Fn. 34 und den Hinweis auf die Auffassung von Lewinski, DuD 2000, 39, 40, der die Überlegung anstellt, eine Gleichbehandlung von Wirtschaftssubjekten dadurch zu erreichen, indem Einzelkaufleute und Freiberufler aus dem Schutzbereich der Datenschutzgesetze herausgenommen werden.

[1055] Vgl. Gola/Schomerus, BDSG, § 43 BDSG Rn. 26; Schaffland/Wiltfang, BDSG, § 43 BDSG Rn. 36 ff.

[1056] Siehe zu „eigenem Geschäftszweck“ die Ausführungen auf S. 208.

[1057] Das Verarbeiten gemäß § 3 Abs. 4 Nr. 3 BDSG umfasst auch das Übermitteln, und zwar das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass an den Dritten die Daten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereit gehaltene Daten einsieht oder abruft.

§ 17 UWG[1058] regelt zwar die strafrechtliche Verantwortung bei Geheimnisverrat auch für die Geschäfts- und Betriebsgeheimnisse von juristischen Personen, aber die Bejahung eines strafbaren Verhaltens bei Aufhebung der Verschlüsselungstechnik oder Weitergabe des Datenschlüssels an einen Dritten unterliegt Einschränkungen. Denn eine Strafbarkeit gemäß § 17 Abs. 2 Nr. 2 UWG setzt voraus, dass sich der Täter ein Geschäfts- und Betriebsgeheimnis unbefugt verschafft oder gesichert hat und dieses unbefugt verwertet oder jemanden mitteilt.[1059] Bei nicht verkörperten Geheimnissen, wie etwa einem Datenschlüssel, der auf keinem Datenträger fixiert ist, bedeutet Sichverschaffen die Kenntniserlangung.[1060] Jedoch erfolgt eine solche Kenntniserlangung nicht unbefugt, da der Provider mit der Einwilligung[1061] des VPN-Auftraggebers das Systemmanagement durchführt.
Eine Strafbarkeit käme allenfalls dann in Betracht, sofern der Provider allein die Wartung des Systems vornehmen würde und dann in unberechtigter Weise in die Verschlüsselungstechnik eingreifen würde. Ist der Provider aber gerade mit dem Systemmanagement und dem Sicherheitsmanagement bzw. der Datenverschlüsselung betraut, so verschafft er sich den generierten Datenschlüssel nicht unbefugt. Abweichend von § 17 Abs. 1 UWG heißt es in § 17 Abs. 2 Nr. 2 UWG nicht, dass strafbares Verhalten dann vorliegt, wenn ein Täter ein Betriebs- und Geschäftsgeheimnis einem Dritten unbefugterweise mitteilt. Für Absatz 2 dieser gesetzlichen Regelung ist vielmehr Voraussetzung, dass Täter sich dieses Geheimnis zunächst unbefugt verschafft und anschließend einem Dritten unbefugt mitteilt.[1062]
Wenn der Provider jedoch über die Geschäfts- und Betriebsgeheimnisse berechtigterweise verfügen darf, diese beim Schlüsselmanagement eines VPN sogar „erschaffen“ darf, so handelt er nicht unbefugt, sondern allenfalls

[1058] Das UWG (Gesetz gegen den unlauteren Wettbewerb)-Reformgesetz ist am 08.07.2004 (BGBl. I S. 1414) in Kraft getreten und enthält eine grundlegende Modernisierung des Lauterkeitsrechts, vgl. hierzu etwa Dieselhorst/Schreiber, CR 2004, 680 ff.; Nuthmann, ITRB 2004, 193, 193.).
[1059] Vgl. Hefermehl/Köhler/Bornkamm, UWG-Kommentar, § 17 UWG Rn. 40 ff.; Harte-Bavendamm/Henning-Bodewig, UWG-Kommentar, § 17 UWG Rn. 31.
[1060] Vgl. auch Köhler in: Köhler/Piper, UWG-Kommentar, § 17 Rn. 26; Harte-Bavendamm/Henning-Bodewig, UWG-Kommentar, § 17 UWG Rn. 20.
[1061] Vgl. zur Rechtswidrigkeit Köhler in: Köhler/Piper, UWG-Kommentar, § 17 Rn. 30.
[1062] Siehe auch Harte-Bavendamm/Henning-Bodewig, UWG-Kommentar, § 17 UWG Rn. 30, die darauf verweisen, dass der gesamte Tatbestand des § 17 Abs. Abs. 2 Nr. 1 UWG erfüllt sein muss.

entgegen der Vorgaben den Anweisungen seines Auftraggebers zweckwidrig, wenn er sich nicht an die Geheimhaltung hält.[1063]
Für ein strafbares Verhalten müsste die Regelung des
§ 17 UWG gerade voraussetzen, dass derjenige bestraft wird, der einem Dritten ein Geschäfts- und Betriebsgeheimnis mitteilt, welches ihm als Auftragnehmer anvertraut worden ist.[1064] Da dies nicht der Fall ist, handelt der Provider nicht unbefugt.

Entsprechendes gilt im Rahmen von § 202a StGB, da auch hier ein strafbares Verhalten nur dann vorliegt, wenn ein Täter unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft.[1065] Nicht für den Täter bestimmt sind Daten, die nach dem Willen des Berechtigten nicht in den Herrschaftsbereich des Täters gelangen sollen.[1066]
Beim Komplettmanagement des Gateway durch den Providerbefindet sich der Schlüssel jedoch gerade in dessen Herrschaftsbereich,[1067] so dass der Provider den Datenschlüssel nicht unbefugt gemäß § 202a StGB ausspäht.[1068]

Zu berücksichtigen ist jedoch, dass eine Strafbarkeit gemäß § 17 Abs. 2 Nr. 2 UWG oder § 202a StGB damit bejaht werden könnte, indem dem Provider unterstellt wird, dass er sich bereits durch Aufhebung der Verschlüsselung die verschlüsselten Daten unbefugt verschafft oder gesichert hat bzw. im Sinne von

[1063] Vgl. Harte-Bavendamm/Henning-Bodewig, UWG-Kommentar, § 17 UWG Rn. 32, die sich auf die Zulässigkeit der Verwertung einwandfrei erlangter Kenntnisse beziehen.
[1064] Vgl. zum Merkmal „Anvertraut“ Harte-Bavendamm/Henning-Bodewig, UWG-Kommentar, § 17 UWG Rn. 9.
[1065] Auch Datenverschlüsselungen sind Sicherungen im Sinne von § 202a StGB (vgl. Tröndle/Fischer, StGB, § 202a StGB Rn. 8).
[1066] Lackner/Kühl, StGB, § 202a StGB Rn. 3; Lenckner in: Schönke/Schröder, StGB, § 202a StGB Rn. 6; Graf in: Münchener Kommentar zum Strafgesetzbuch, § 202a StGB Rn. 49 (zum Merkmal „unbefugt“). Auch Tröndle/Fischer, StGB, § 202a StGB Rn. 7 verweisen darauf, dass die zweckwidrige Verwendung von für den Täter bestimmten Daten nicht erfasst ist.
[1067] Vgl. zum Komplettmanagement durch den Provider S. 49.
[1068] Siehe im Übrigen Ernst, CR 2003, 898 ff. zur Frage der Strafbarkeit des „Abhörens“ ungesicherter Kommunikation gemäß § 202a StGB. Ernst, CR 2003, 898, 899, verweist darauf, dass es für die besondere Sicherung gemäß § 202a StGB nicht darauf ankommt, welche Art der Verschlüsselung gewählt wird (in dem Sinne, ob diese leicht aufzuheben oder umgangen werden kann), da der Verfügungsberechtigte durch diese Sicherung nur sein Interesse an der Geheimhaltung dokumentieren muss. Siehe aber auch Dornseif/Schumann/Klein, DuD 2002, 226, 229 ff.

§ 202a StGB einem Dritten verschafft hat.[1069] Sofern dem Provider keine Zugriffsrechte oder das Recht zur Kenntnisnahme bezüglich der unverschlüsselten Daten zustehen, handelt er unbefugt.[1070] Die unbefugte Mitteilung an einen Dritten würde in diesem Falle in einem Unterlassen der Datensicherung bestehen.[1071] In diesem Falle müsste sich der Blickpunkt also auf die unbefugte Kenntnisnahme der (unverschlüsselten) Daten richten: Hebt der Provider die Verschlüsselung auf bzw. leitet er die Daten unverschlüsselt weiter, so erfüllt er nicht seine Verpflichtung zur Datensicherung.
Zu berücksichtigen ist allerdings, dass dieses Argument dann nicht zum Tragen kommt, sofern der VPN-Auftraggeber mit der Entschlüsselung der Daten einverstanden ist. Übernimmt der Provider das komplette Schlüsselmanagement, so kann die Aufhebung der Verschlüsselung auf dem Gateway und die (unverschlüsselte) Datenweiterleitung ins lokale Netzwerk des VPN-Auftragnehmers gerade Vertragsbestandteil sein.[1072] Damit verschafft sich der Provider ebenso wenig unbefugt Kenntnis über die Daten bzw. über ein Geheimnis.

Um Strafbarkeitslücken zu vermeiden, bedarf es damit entweder in rechtspolitischer Hinsicht einer Gleichstellung zwischen personenbezogenen Daten und Geschäfts- und Betriebsgeheimnisses, sofern ein Provider mit dem Komplettmanagement eines Gateway betraut ist und Daten rechtmäßig bzw. vertragsgemäß entschlüsseln darf. Dem VPN-Auftraggeber steht es aber alternativ (im Sinne eines Selbstdatenschutzes) ebenso frei, die vertraglichen Regelungen derart auszugestalten, dass er den Provider zur (ausschließlich) verschlüsselten Weiterleitung verpflichtet oder auf diese VPN-Variante verzichtet.

[1069] Vgl. Harte-Bavendamm/Henning-Bodewig, UWG-Kommentar, § 17 UWG Rn. 20. Vgl. auch Lenckner in: Schönke/Schröder, StGB, § 202a StGB Rn. 10; Graf in: Münchener Kommentar zum Strafgesetzbuch, § 202a StGB Rn. 43/44.
[1070] Siehe Hefermehl/Köhler/Bornkamm, UWG-Kommentar, § 17 UWG Rn. 43, wo dargelegt wird, dass unbefugtes Handeln vorliegt, wenn dem Täter kein Rechtfertigungsgrund (z.B. Einwilligung) zur Seite steht und das Geheimnis auch nicht offenkundig geworden ist.
[1071] Zur unbefugten Mitteilung durch Unterlassen siehe Harte-Bavendamm/Henning-Bodewig, UWG-Kommentar, § 17 UWG Rn. 10. Siehe auch Hefermehl/Köhler/Bornkamm, UWG-Kommentar, § 17 UWG Rn. 19, wo darauf verwiesen wird, dass das pflichtwidrige Unterlassen bzw. das Dulden der Kenntnisnahme dem positiven Tun gleichsteht.
[1072] Siehe Böhmer, Virtual Private Networks, S. 217/248 (1. Auflage), der darauf verweist, dass der Weg vom Gateway zum Endgerät unverschlüsselt erfolgt (in diesem Sinne ebenso in der 2. Auflage, S. 225). Siehe außerdem S. 47 in dieser Arbeit und Fn. 208.

cc. Technische Schutzmaßnahmen

Hat ein Provider die Funktionsherrschaft über den Gateway inne, sind im Rahmen der datenschutzrechtlichen Prüfung ebenso die ihm obliegenden technischen Schutzmaßnahmen zu berücksichtigen.

Dabei sind die nachfolgenden VPN-Varianten zu berücksichtigen:

- Komplettmanagement des Providers[1073]
- Splitmanagement im Machtbereich des Providers[1074]

Zu prüfen ist, welche Unterrichtungs- und Verschlüsselungspflichten den Provider treffen.

aaa. Unterrichtungspflichten des Providers über Netzsicherheit

Erbringt der Provider durch den Betrieb des Gateways einen eigenen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG bzw. wirkt er daran mit[1075] hat er die Funktionsherrschaft über den Gateway als Telekommunikationsanlage inne und ist Diensteanbieter gemäß § 3 Nr. 6 TKG. Auf dem Gateway werden die Daten entschlüsselt und an das lokale Netzwerk weitergesendet.[1076] Der Gateway, auf dem die Sicherheitsfunktionen implementiert sind, steht im Einflussbereich des Providers, der den alleinigen Einfluss auf den Betrieb oder Nichtbetrieb hat. Von diesem Gateway aus wird der Datenverkehr in das Netzwerk des VPN-Auftraggebers weitergeleitet, wobei die Weiterleitung über eine Punkt-zu-Punkt-Verbindung und nicht weiterhin über das Internet erfolgt.[1077]

[1073] Siehe S. 49.
[1074] Siehe S. 52.
[1075] Vgl. hierzu oben S. 154.
[1076] Siehe Böhmer, Virtual Private Networks (2. Auflage), S. 217/248, der darauf verweist, dass der Weg vom Gateway zum Endgerät unverschlüsselt erfolgt (1. Auflage). In diesem Sinne ebenso Böhmer in der 2. Auflage, S. 225). Vgl. außerdem das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 216. Siehe außerdem S. 47 und Fn. 208.
[1077] Siehe S. 49. Siehe hierzu auch das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 239 ff.

Insoweit ist der Provider gemäß § 109 Abs. 1 TKG und Artikel 4 der EU-Richtlinie 2002/58/EG zur umfassenden Aufklärung über mögliche Sicherheitsrisiken verpflichtet.[1078] Diese Verpflichtung trifft ihn allein aufgrund des Umstandes, dass er die Funktionsherrschaft über den Gateway innehat und gilt daher gleichermaßen für die VPN-Varianten des Komplettmanagement und des Splitmanagement in seinem Machtbereich.[1079]
Erwägungsgrund 20 der EU-Richtlinie 2002/58/EG enthält hierzu im Übrigen als beispielhaft aufgezählte Maßnahme die Informationspflicht der Nutzer und Teilnehmer über Maßnahmen zum Schutz der von ihnen übertragenen Nachrichten, wie z.B. den Einsatz spezieller Software oder von Verschlüsselungstechniken. Insoweit ergibt sich hier ebenso eine Überschneidung zu den Pflichten aus § 93 TKG.[1080]

Derzeit wird darauf verwiesen, dass das Tunneling-Protokoll IPSec das sicherste Verschlüsselungsprotokoll im Rahmen eines VPN darstellt.[1081] Daher stellt sich die Frage, ob der Internetzugangs-Provider, der einen weiteren Telekommunikationsdienst durch das Management bzw. Betrieb des Gateways (auf dem die Tunneling-Technik implementiert ist) erbringt bzw. daran mitwirkt, verpflichtet ist, dem VPN-Auftraggeber im Sinne des Artikels 4 Abs. 2 und des Erwägungsgrundes 20 der EU-Richtlinie 2002/58/EG dringend zu empfehlen, dieses Protokoll im Rahmen eines VPN zu nutzen bzw. über entsprechende gleichwertige Protokolle aufzuklären.[1082] Problematisch ist, dass noch andere

---

[1078] Siehe hierzu die Ausführungen auf S. 110 ff.
[1079] Zur bildlichen Darstellung soll nochmals auf S. 49 (Komplettmanagement) und S. 52 (Splitmanagement) verwiesen werden sowie auf die rechtlichen Ausführungen auf S. 156.
[1080] Siehe hierzu die Ausführungen auf S. 110 ff.
[1081] Siehe S. 39 ff. Siehe aber auch die Ausführungen in der Computerwoche vom 21.01.2006 (http://whitepaper.computerwoche.de/index.cfm?pid=1&fk=61&pk=466) mit dem Hinweis, dass sich seit geraumer Zeit Zeitschriftenbeiträge über IPSec häufen. In diesen Artikeln sei immer wieder die Rede davon, dass IPSec der höchste Sicherheits-Standard und das für jede Netzwerk-Topologie uneingeschränkt einsetzbare VPN-Protokoll sei. Die Autoren möchten in ihrem Beitrag jedoch zeigen, dass IPSec nur in ganz bestimmten Umgebungen ohne zusätzliche Erweiterungen eingesetzt werden kann.
[1082] Koenig/Röder, CR 2000, 668, 671 beziehen sich in ihren Ausführungen auf die Telekommunikations-Datenschutzrichtlinie, die von der EU-Richtlinie 2002/58/EG abgelöst worden ist (siehe Fn. 844), und merken an, dass nach Artikel 4 der Telekommunikations-Datenschutzrichtlinie Internet-Diensteanbieter verpflichtet sind, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten, insoweit davon die Netzsicherheit betroffen ist, nötigenfalls zusammen mit dem Betreiber der zugrunde liegenden Netzinfrastruktur. Gleichlautendes regelt Artikel 4 der EU-Richtlinie 2002/58/EG. Bei der Datensicherheit sind der Stand der Technik und die Kosten der Sicherungsmaßnahmen zu berücksichtigen (Koenig/Röder, aaO), wobei der Telekommunikationsanbieter über das Risiko der Verletzung der Netzsicherheit sowie über

Produkte auf dem Markt sind, wie das ebenfalls erwähnte Protokoll PPTP, L2Sec oder L2TP. PPTP ist von Microsoft entwickelt worden, wobei PPTP im Hinblick auf die Sicherheit der Verschlüsselung als sehr unsicher eingestuft werden muss und L2TP erst gar keine Verschlüsselung bietet.[1083] Daher besteht darüber hinaus die Unsicherheit, ob tatsächlich von den Providern erwartet werden kann, umfassend über die Betriebssicherheit aufzuklären. Dies liefe im Einzelfall eventuell darauf hinaus, eigene Produkte nicht zu empfehlen. Die Antwort auf diese Fragestellungen ergibt sich jedoch eindeutig aus der Intention des Artikels 4 und des Erwägungsgrundes 20 der EU-Richtlinie 2002/58/EG, in dessen Sinne - als europarechtliche Vorgabe - auch § 109 Abs. 1 TKG auszulegen ist: Der Teilnehmer ist über die Betriebssicherheit umfassend aufzuklären. Dazu gehört ebenso die Information über Nachteile und Schwächen von den angebotenen Diensten und über den Einsatz spezieller Software oder von Verschlüsselungstechniken, wobei auf die Unterrichtung über alle besonderen Risiken der Verletzung der Netzsicherheit abgestellt wird, und der Diensteanbieter die Teilnehmer und Nutzer unbedingt vollständig über die Sicherheitsrisiken aufklären muss, gegen die er selbst keine Abhilfe bieten kann.

Wenn nun ein Diensteanbieter also wie hier in die Bereitstellung eines VPN derart eingebunden ist, dass er einen über die reine Bereitstellung des Internetzugangs hinausgehenden Telekommunikationsdienst gemäß § 3 Nr. 24 TKG erbringt, dann ist er ebenso verpflichtet, über die spezielle VPN-Technik und VPN-Protokolle zu unterrichten. Angemessene Unterrichtung kann der Provider allerdings nur dann durchführen, sofern er Kenntnis über die seitens des VPN-Auftraggebers geplante Verwendung hat. Denn nur dann kann er abschätzen, wo die besonderen Risiken der Netzunsicherheit liegen. Das Fernmeldegeheimnis, welches sich gemäß § 88 TKG ebenso auf den Inhalt der Kommunikation bezieht, kann weniger stark betroffen sein, sofern der VPN-Auftraggeber lediglich auf Daten den Zugriff gewähren bzw. Daten übertragen möchte, die er nicht als besonders schutzbedürftig einschätzt.

mögliche Abhilfen einschließlich der Kosten unterrichten muss. Daher sollte auch der Provider eines VPN dazu verpflichtet sein, den Kunden eingehend über die möglichen Verschlüsselungsmethoden und deren Vor- und Nachteile aufzuklären (siehe diesbezüglich ebenso die Ausführungen auf S. 235 ff.).

[1083] Siehe oben S. 35 ff.

Es kann in diesem Zusammenhang auch die Erwartungshaltung des VPN-Auftraggebers für die Reichweite und Angemessenheit der Aufklärungspflichten von entscheidender Bedeutung sein. Sofern der VPN-Auftraggeber mit dem Begriff „Tunnel“ Datensicherheit gleichsetzt,[1084] so kommt es ihm hauptsächlich auf eine wirksame und effektive Verschlüsselung seiner Daten an.

Es ist aber ebenso möglich, dass der VPN-Auftraggeber überwiegend sein Netzwerk vor unberechtigten Zugriffen sichern möchte, aber mangels besonderer Schutzbedürftigkeit der zur Übertragung vorgesehenen Daten weniger großen Wert auf besonders starke Verschlüsselungen legt. In diesem Falle ist dem VPN-Auftraggeber mehr an einer effektiven und sicheren Authentifizierungsmöglichkeit gelegen, damit nicht unberechtigte Dritte ein „Schlupfloch“ in sein Firmennetz finden. Im Besonderen ist hier zu berücksichtigen, dass es technische Grenzen für die Verwirklichung eines VPN gibt. Nutzt der VPN-Auftraggeber an seinen Standorten kein IP-Netzwerk, so kann er keine Datenverschlüsselungen mittels IPSec vornehmen.[1085] Daher muss sich die Angemessenheit der Verschlüsselungsmaßnahmen hier nach anderen Kriterien richten, insbesondere der technischen Machbarkeit unter Berücksichtigung der Kosten.

Es muss daher unter Einbeziehung der geplanten Verwendung durch den VPN-Auftraggeber entschieden werden, welches Protokoll oder Technik, auch im Hinblick auf die Möglichkeiten von Zertifizierungen, am besten für dessen Zwecke geeignet ist.[1086]
Es müssen nicht alle erdenklichen technischen Maßnahmen getroffen werden.[1087] Sofern der Kunde aber ein besonderes Interesse an der Datensicherheit hat und nicht nur eine kostengünstige Verbindung weit entfernter Standorte vornehmen möchte,[1088] ist der Schutzaufwand davon abhängig, in welchem Umfange der Benutzer davon ausgehen darf, dass sein

[1084] Vgl. auch Schneider, MMR 1999, 571, 575. Siehe hierzu auch die Ausführungen auf S. 35 ff. in dieser Arbeit zu den unterschiedlichen Möglichkeiten eines VPN:
[1085] Siehe hierzu S. 39 ff.
[1086] Vgl. auch Zimmer, CR 2003, 893, 896 ff.; Zerres in: Scheurle/Mayen, TKG-Kommentar, § 87 TKG Rn. 17 ff.; Trute in: Trute/Spoerr/Bosch, TKG-Kommentar, § 87 TKG Rn. 14.
[1087] Vgl. Ehmer in: TKG-Kommentar (2. Auflage), § 87 TKG Rn. 24/29; Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 22; Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 87 TKG(1998), Band 1, Rn. 9.
[1088] Siehe zu den Gründen für die Verwendung von Tunneling-Protokollen S. 33 ff.

Fernmeldegeheimnis gewahrt wird und Dritten die Möglichkeit eines Eingriff erschwert wird.[1089] Er hat in diesem Falle ein besonderes Interesse, die Kenntnisnahme durch unbefugte Dritte zu verhindern.

Dementsprechend muss mittels des Expertenwissens des Providers und der voraussichtlichen Kosten abgeschätzt werden,[1090] ob und wie für den VPN-Auftraggeber die Datensicherheit zu bewerkstelligen ist. Da die jeweiligen Schutzmaßnahmen auch von den konkret angebotenen Telekommunikationsdiensten abhängig sind,[1091] ist daher die aktuelle VPN-Technik seitens des Providers in diese Überlegungen mit einzubeziehen.

Die Unterrichtungspflichten über Verschlüsselungstechniken und spezieller Software sind im Übrigen bei Backbone-Betreibern[1092] von besonderer Bedeutung, da diese teilweise damit werben, eine spezielle Technik namens MPLS[1093] und einzusetzen und dies als besonderes Datensicherheitsmerkmal bei VPN anbieten.[1094] Hierbei ist aber zu berücksichtigen, dass die MPLS-Technik durch die Hinzufügung eines MPLS-Headers vorrangig eine Verbesserung der Performance, des Datendurchsatzes, bietet, aber allein die Hinzufügung dieses weiteren Headers keine Verschlüsselung des Dateninhalts ermöglicht.[1095] Der Provider ist daher verpflichtet, darüber zu unterrichten, inwieweit MPLS dennoch zu Verschlüsselungsprotokollen, wie beispielsweise IPSec, einen gleichwertigen Schutz bieten kann, oder ob

[1089] Vgl. Ehmer in: TKG-Kommentar (2. Auflage), § 87 TKG Rn. 24; vgl. auch Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 22.
[1090] Vgl. auch die Ausführungen auf S. 199.
[1091] Siehe Ehmer in: TKG-Kommentar (2. Auflage), § 87 TKG Rn. 29; siehe auch Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 21, der darauf verweist, dass der Stand der Technik zu berücksichtigen ist.
[1092] Siehe zu diesem Begriff Petri/Göckel, CR 2002, 329 ff. sowie S. 28 ff. in dieser Arbeit.
[1093] Siehe zu MPLS auch Buckbesch/Köhler, Virtuelle Private Netze, S. 122 sowie die Ausführungen auf S. 34 ff. (insbesondere auch Fn. 141) sowie S. 197 in dieser Arbeit.
[1094] MPLS wird beispielsweise angeboten von COLT TELECOM GmbH abrufbar unter http://www.colt.net/de/ge/produkte/data_/colt_ip_vpn_corporate; Arcor AG & Co.KG abrufbar unterhttp://www.arcor.de/business/enterprise/fnetz/net_det.jsp ; Cable & Wireless Telecommunication Services GmbH abrufbar http://www.cw.com/europe/services/carrier_mpls.html;
Claranet GmbH abrufbar unter http://www.claranet.de./ipservices/vpn/vpn_mpls.php (alle Websites vom 30.09.2006).
[1095] Siehe S. 34 in dieser Arbeit.

Verschlüsselungsprotokolle zur Optimierung der Datensicherheit zusätzlich eingesetzt bzw. mit MPLS kombiniert werden sollten.[1096]

Entsprechendes gilt im Hinblick auf das im technischen Teil dargestellte Schlüsselaustausch-Protokoll IKE.[1097] In den dortigen Ausführungen ist ebenso darauf hingewiesen worden, dass dies zwar regelmäßig bei IPSec eingesetzt wird, es aber auch noch weitere Standards bezüglich eines Schlüsselmanagements gibt.[1098] Der technisch nicht versierte VPN-Auftraggeber hat keine Ahnung, wo die Unterschiede der unterschiedlichen Protokolle liegen, die Auswirkungen auf die Sicherheit seines VPN haben. Es gibt insbesondere mehrere IPSec-fähige Produkte unterschiedlicher Hersteller.[1099] Daher ist auch hier eine Aufklärung und Information erforderlich.

Der Provider muss ebenso über den Umstand informieren, falls die Datenweiterleitung vom Gateway in das lokale Netz des VPN-Auftraggebers unverschlüsselt erfolgt,[1100] sowie darüber, ob und inwiefern dies Auswirkungen auf die Datensicherheit hat bzw. wie Abhilfe zu schaffen ist. So wird teilweise die Datenübertragung über die Telefonleitung als ein Umstand angesehen, der keine besondere Datenverschlüsselung erfordert.[1101]
Diese Hinweispflicht gilt im Übrigen unter Berücksichtigung des Artikels 4 Abs. 2 der EU-Richtlinie 2002/58/EG ebenso, sofern die der Datenübertragung zugrunde liegende physische Leitung von einem anderen Provider betrieben wird bzw. ein anderer Provider die Funktionsherrschaft über die Leitung

[1096] Siehe hierzu insbesondere die vergleichende Aufstellung zwischen IPSec und MPLS, abrufbar unter http://www.claranet.de./ipservices/vpn/
[1097] Vgl. oben S. 42.
[1098] Vgl. S. 42 unter Verweis auf Campo/Pohlmann, Virtual Private Networks, S. 165/166.
[1099] Campo/Pohlmann, Virtual Private Networks, S. 151.
[1100] Siehe hierzu das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 236 ff. Siehe außerdem Böhmer, Virtual Private Networks (1. Auflage), S. 217/248, der darauf verweist, dass der Weg vom Gateway zum Endgerät unverschlüsselt erfolgt (in diesem Sinne ebenso Böhmer in der 2. Auflage, S. 225). Siehe außerdem Campo/Pohlmann, Virtual Private Networks, S. 136 ff. Vgl. auch das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 216 mit dem Hinweis, dass das VPN-Gateway den mittels IPSec neu eingefügten IP-Header entfernt, entschlüsselt und die Daten in das lokale Netzwerk sendet.
[1101] Vgl. insbesondere Buckbesch/Köhler, Virtuelle Private Netze, S. 112, die feststellen, dass leider im Falle von Standleitungen immer noch suggeriert wird, dass diese privat und daher „sicher" sind. Dies ist aber nicht richtig, da diese Leitungen nur Bestandteil des öffentlichen (Telekom-)Netzes sind, und vor allem sehr einfach physikalisch anzapfbar und damit in keiner Weise dem Anspruch der Datensicherheit genügen (Buckbesch/Köhler, aaO). Daher ist auch im Falle einer (Telefon-)Leitung von Gateway zum Firmennetz allein durch die Leitung keine Sicherheit der Daten gegeben, sondern es müsste vielmehr eine zusätzliche Verschlüsselung erfolgen.

innehat. Anderenfalls müsste der Provider gemäß § 109 Abs.1 TKG und Artikel 4 Abs. 2 der EU-Richtlinie 2002/58/EG sowie deren Erwägungsgrund 20 wiederum über mögliche Abhilfen oder erneut verschlüsseln informieren.

Hieran ist gut zu erkennen, dass ein Systemmanagement in dem hier beschriebenen Sinne für den Provider erheblich mehr Pflichten bedeutet, da er nicht nur eine Auftragsdatenverarbeitung übernimmt, sondern er vielmehr Anbieter eines Telekommunikationsdienstes gemäß § 3 Nr. 6 TKG ist. Daraus folgt auch, dass er gemäß § 44 TKG Schadensersatzansprüchen ausgesetzt sein kann, sofern die von ihm vorgenommenen Schutzmaßnahmen nicht angemessen sind.[1102]
Insbesondere ist, wie gerade angesprochen, zu bedenken, dass die einzelnen Sicherheitsmaßnahmen, die ein Provider zu treffen hat, im besonderen Maße von dem Ziel und der Verwendung des VPN durch den Kunden abhängen. Ein Provider kann erst dann die notwendigen und angemessenen Vorkehrungen treffen und die entsprechenden Verschlüsselungen einsetzen, sofern ihm bekannt ist, welche Anforderungen der VPN-Auftraggeber an die Sicherheit stellt bzw. welchen datenschutzrechtlichen Verpflichtungen er gegebenenfalls unterliegt. So wäre vorstellbar, dass der VPN-Auftraggeber das VPN gegebenenfalls nur Externen zur Verfügung stellen möchte, damit diese ihre personenbezogenen Daten übertragen können.[1103] In diesem Falle könnten gegebenenfalls andere Verschlüsselungen in Betracht kommen, was aber erst durch Berücksichtigung des Personenverhältnisses zwischen VPN-Auftraggeber und Betroffenem oder Nutzer festgestellt werden kann.

[1102] Siehe zur Schwierigkeit des Nachweises eines konkreten Schadens in der Praxis Groß in: Roßnagel, Handbuch Datenschutzrecht, 7.8 Rn. 56 unter Verweis auf Büchner in: TKG-Kommentar (2. Auflage), § 40 TKG Rn. 9. Zu berücksichtigen ist aber, dass im Zusammenhang mit mangelnden Verschlüsselungstechniken, etwa auch im Hinblick auf die Aufdeckung von geheimen Know-How, wie beispielsweise noch nicht veröffentlichte Patentanmeldungen, unter Umständen ein Schaden eher nachweisbar sein kann.
[1103] Vgl. zum Extranet-VPN S. 2.

bbb. Verschlüsselung

Die obigen Ausführungen zur Aufklärungspflicht eines Providers über die Netzsicherheit (im Rahmen eines Komplettmanagement[1104] oder Splitmanagement[1105] des Gateway) sind um die Frage zu ergänzen, inwieweit ihm bei diesen VPN-Varianten darüber hinaus selbständige Verschlüsselungsmaßnahmen obliegen.

(1) Komplettmanagement des Providers

Sofern der Provider das Komplettmanagement des Gateway übernimmt, erbringt er einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG, da er in rechtlicher und tatsächlicher Hinsicht die Kontrolle über den Gateway innehat.[1106]
Beim Komplettmanagement des Gateway[1107] hat der Provider es daher ebenso in der Hand hat, selbständig für die Verschlüsselung der Daten zu sorgen. Erist derjenige, der die Sicherheit auf dem Gateway sicherzustellen hat, und die Verschlüsselungstechnik auf dem Gateway bereitstellt.
Folglich ist der Provider in diesem Falle nicht nur zur Unterrichtung über die Verschlüsselung gemäß § 109 Abs. 1 TKG verpflichtet, sondern er muss auch für deren entsprechenden Einsatz bzw. Verwendung sorgen.[1108]

(2) Splitmanagement im Machtbereich des Providers

Beim Servicemanagement bzw. Splitmanagement[1109] des Gateway im Einfluss- bzw. Machtbereich des Providers kann der Provider hingegen nur die Aufklärung und Unterrichtung gemäß § 109 Abs. 1 TKG über die unterschiedlichen Verschlüsselungen übernehmen. Er ist nicht für den Einsatz der Verschlüsselungstechnologien verantwortlich, sonderndie entsprechende

[1104] Siehe S. 49.
[1105] Siehe S. 52.
[1106] Siehe zur Funktionsherrschaft S. 149 ff. Vgl. zur rechtlichen und tatsächlichen Kontrolle auch Bothe/Heun/Lohmann, ArchivPT 1995, 5, 18/20.
[1107] Vgl. hierzu das Bildbeispiel auf S. 49.
[1108] Vgl. hierzu S. 113 ff. Vgl. außerdem die Ausführungen von Koenig/Röder, CR 2000, 668 ff.
[1109] Siehe hierzu das Bildbeispiel auf S. 52. Siehe zu den Unterrichtungspflichten über die Netzsicherheit die Ausführungen auf S. 110 ff.

Verwendung oder Nichtverwendung der Verschlüsselung im Einzelfall ist dem VPN-Auftraggeber vorbehalten. Der VPN-Auftraggeber kann durch entsprechende Administrationsrechte (mittels Fernzugriff) selbständig über die Sicherheitsstrategie entscheiden.[1110]

In diesem Zusammenhang ist im Besonderen nochmals auf die rechtlichen Unterschiede im Rahmen des Splitmanagement aufmerksam zu machen: Die zwei denkbaren Varianten des Splitmanagement[1111] erfahren eine unterschiedliche rechtliche Beurteilung, je nachdem in welchem Machtbereich der Gateway steht.
Obwohl der Provider sowohl beim Splitmanagement im Firmennetz bzw. Machtbereich des VPN-Auftraggebers als auch beim Splitmanagement im Machtbereich des Providers „nur" ein Servicemanagement durchführt, ergeben sich doch unterschiedliche rechtliche Bewertungen. Nur wenn der Gateway im Machtbereich des Providers steht, obliegen ihm gesetzliche Aufklärungspflichten über die Netzsicherheit gemäß § 109 Abs. 1 TKG. Denn in diesem Falle erbringt der Provider selbst einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG, da er die Funktionsherrschaft über den Gateway innehat.[1112]
Es werden zwar seitens des Providers lediglich die Service- und die Wartungsarbeiten übernommen, während der VPN-Auftraggeber die Benutzerverwaltung und das gesamte Sicherheitsmanagement bzw. Schlüsselmanagementbetreut Aber der Provider erbringt dennoch ein „Mehr", da er nicht nur einen Internetzugangsknoten bereitstellt, sondern für das VPN einen weiteren eigenständigen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG erbringt und damit den entsprechenden Verpflichtungen gemäß §§ 91 ff. TKG unterliegt. Der Provider leistet auch im Vergleich zum Splitmanagement im Machtbereich des VPN-Auftraggebers mehr. Ein solches Servicemanagement des Providers führt gerade nicht zur Einordnung dieser Leistung als

[1110] Siehe hierzu das Bildbeispiel auf S. 52. Siehe zu den Unterrichtungspflichten über die Netzsicherheit die Ausführungen auf S. 110 ff.
[1111] Siehe hierzu S. 51 (Gateway steht im Machtbereich des VPN-Auftraggebers) und S. 52 (Gateway steht im Machtbereich des Providers).
[1112] Siehe zu dieser rechtlichen Einordnung bereits die Ausführungen auf S. 156 ff. Vgl. auch Schütz in: TKG-Kommentar (2. Auflage), § 6 TKG Rn. 34, derselbe in: TKG-Kommentar (3. Auflage), § 16 Rn. 23 und Manssen in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 3 TKG(1998), Band 1, Rn. 3 zur Funktionsherrschaft.

Telekommunikationsdienst gemäß § 3 Nr. 24 TKG,[1113] so dass dem Provider dementsprechend keine besonderen Pflichten nach § 109 Abs. 1 TKG obliegen.[1114]

Es kann zwar die Frage gestellt werden, ob es im Hinblick auf die Konsequenzen gerechtfertigt ist, ausschließlich danach zu unterscheiden, an welchem Ort der Gateway steht. Aber dies ist letztendlich nicht entscheidend. Denn Anknüpfungspunkt ist allein, ob der Provider aufgrund des Managements des Gateway gemäß § 3 Nr. 6 TKG Anbieter eines Telekommunikationsdienstes ist.
Letzteres kommt dann nicht in Betracht, wenn er nur den Service im Firmennetz des Kunden übernimmt oder ein Software-VPN bereitstellt. Ein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG liegt nur vor, wenn der Provider durch die Bereitstellung eines in seinem Machtbereich stehenden Gateway ein VPN bereitstellt bzw. daran im Sinne von § 3 Nr. 6b) TKG mitwirkt. Dies geht über die Zurverfügungstellung eines Internetzugangsknotens hinaus. Auch wenn der VPN-Auftraggeber im Endeffekt eigenständig für den Einsatz der entsprechenden Benutzerverwaltung und Verschlüsselungstechnik verantwortlich ist, ist der Provider nicht davon entbunden, entsprechende VPN-spezifische Aufklärung zu leisten. Dies zählt gemäß § 109 Abs. 1 TKG unter Berücksichtigung von Artikel 4 Abs. 2 der EU-Richtlinie 2002/58/EG zu seinen angemessenen Schutzvorkehrungen „dieses“ Telekommunikationsdienstes. Es betrifft eine Schutzmaßnahme, die außerhalb des eigentlichen Geltungsbereiches der von ihm zu treffenden Maßnahmen liegt, über welche er aber dennoch als Telekommunikationsdiensteanbieter dieses „Teil“-Dienstes des VPN aufklären muss.

[1113] Siehe zu dieser rechtlichen Einordnung bereits die Ausführungen auf S. 152 ff.
[1114] Siehe zu dieser rechtlichen Einordnung bereits die Ausführungen auf S. 231 ff.

ccc. Anforderungen an den Gateway

Im Hinblick auf den Gateway hat der Provider darüber hinaus die Anforderungen des § 109 Abs. 2 und Abs. 3 TKG zu beachten, sofern der Gateway einer Vielzahl von Teilnehmern zur Verfügung steht und nicht nur einem einzigen Kunden. Denn ein Provider wird regelmäßig nicht unzählig viele Hardware-Geräte (Gateways) einsetzen, sofern auf einem physischen Gerät die logische Trennung der Teilnehmer möglich ist. Die in § 109 Abs. 2 und Abs. 3 TKG geregelten Verpflichtungen gelten unabhängig davon, ob es sich um ein Splitmanagement oder um ein Komplettmanagement des Gateways handelt, da allein die Funktionsherrschaft über den Gateway entscheidend ist. Ausschlaggebend ist, dass ein Telekommunikationsdienst für die Öffentlichkeit erbracht wird.[1115] Insoweit besteht also eine Parallele zu dem Prüfungspunkt „Unterrichtungspflichten des Providers über die Netzsicherheit".[1116]

Zu berücksichtigen ist aber, dass der Provider zwar einen Telekommunikationsdienst für die Öffentlichkeit erbringt, sofern an seinem Gateway eine Vielzahl von Kunden (und nicht nur ein von der Allgemeinheit abgrenzbarer Personenkreis) angeschlossen ist.[1117] Dennoch gehört zu einem schriftlichen Sicherheitskonzept gemäß § 109 Abs. 3 TKG nicht zwangsläufig die Darstellung von Authentifizierungsmaßnahmen oder Verschlüsselungsprotokollen im Hinblick auf jeden einzelnen Kunden.[1118] Dies stellen vielmehr Maßnahmen dar, die den Provider gemäß § 109 Abs. 1 TKG treffen, da die jeweilige Benutzerverwaltung und Verschlüsselung für den einzelnen Kunden individuell erarbeitet werden kann und von dessen Verwendung abhängt. Es ist nicht die Sicherheit des Gateway „als Ganzes und für die Öffentlichkeit" betroffen und lediglich auf einen einzelnen Kunden bzw. VPN-Auftraggeber bezogene Sicherheitsmaßnahmen stellen daher keinen Bestandteil eines Sicherheitskonzept gemäß § 109 Abs. 3 TKG dar. So muss

[1115] Zum Telekommunikationsdienst für die Öffentlichkeit siehe Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 100 sowie S. 116 ff. in dieser Arbeit.
[1116] Siehe oben S. 234 ff.
[1117] Siehe zur geschlossenen Benutzergruppe S. 117/184 ff. Vgl. Trute/Spoerr/Bosch, TKG-Kommentar, § 3 TKG Rn. 85; siehe auch § 6 Abs. 2 Telekommunikations-Verleihungsverordnung.
[1118] Siehe zum Sicherheitskonzept Zimmer, CR 2003, 896, 898; Heibey in: Roßnagel, Handbuch Datenschutzrecht, 4.5 Rn. 30 sowie die weiteren Ausführungen auf S. 114 in dieser Arbeit.

zwar für den einzelnen Kunden sichergestellt werden, dass ausschließlich berechtigte Personen in dem VPN eingebunden sind und auf die Firmenzentrale Zugriff nehmen können,[1119] wobei sich im Einzelfall die Frage stellen kann, ob die Integrität und Authentizität bei sämtlichen Techniken gleichermaßen gewahrt ist.[1120] Auch ist bei der Datenübertragung die Sicherheit der Daten durch den Einsatz entsprechender Verschlüsselungsprotokolle zu gewährleisten. Aber dies sind einzelfallbezogene Anforderungen und nicht zwangsläufig „für eine Öffentlichkeit“ obligatorisch.

dd. Auskunfts- und Überwachungsmaßnahmen

Bei einer Gesamtbeurteilung von Datenschutz und Datensicherheit ist gleichermaßen zu berücksichtigen, inwieweit diese aufgrund staatlicher angeordneter Überwachung oder Auskunftsverpflichtungen eingeschränkt sein können.[1121]

aaa. Aufhebung der Benutzerauthentifizierung

Der Provider ist nicht nur im Sinne eines manuellen Auskunftsverfahrens gemäß § 113 Abs. 1 S. 1 TKG zur Auskunft über die Daten der §§ 95, 111 TKG verpflichtet. Darüber hinaus ist nunmehr in § 113 Abs. 1 S. 2 TKG geregelt, dass der Telekommunikationsdiensteanbieter ebenso zur Auskunft über Daten gemäß §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO verpflichtet ist, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird, insbesondere PIN und PUK.
Da auch die Benutzerauthentifizierung[1122] auf dem Gateway eine Zugriffsberechtigung im Hinblick auf das Kundennetzwerk darstellt, ist dies mit einem PIN vergleichbar. Im Falle des Komplettmanagement des Gateway durch den Provider ist davon ebenso die Benutzerverwaltung in seinem Netz- bzw. Einflussbereich umfasst.[1123] Als Anbieter eines Telekommunikationsdienstes

[1119] Siehe S. 46 ff.
[1120] Siehe zu den Schwächen von Authentifizierungen auch S. 60, insbesondere Fn. 265. Vgl. zu „Integrität“ und „Authentizität“ außerdem Jacob, DuD 2000, 5, 10.
[1121] Siehe die Darstellung der datenschutzrechtlichen Pflichten auf S. 106 ff. sowie S. 162 ff.
[1122] Vgl. zu den Möglichkeiten der Benutzerauthentifizierung Lipp, VPN, S. 145 ff. sowie S. 59 ff. in dieser Arbeit (zum zwangsweisen Tunneling).
[1123] Vgl. auch Lipp, VPN, S. 398. Siehe außerdem das Bildbeispiel auf S. 49.

gemäß § 3 Nr. 6 TKG ist der Provider gleichermaßen Verpflichteter der in § 113 Abs. 1 S. 2 TKG i.V.m. §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO geregelten Maßnahmen. [1124]

Der Provider ist daher zur Offenlegung der Benutzerauthentifizierungen, da diese im Sinne der gesetzlichen Regelung des § 113 Abs. 1 S. 2 TKG einen Zugriffsschutz (vergleichbar einem PIN) darstellen. Dies kann ebenso die Offenlegung der Nutzer zur Folge haben. Allerdings ist zu beachten, dass die Aufhebung der Benutzerauthentifizierung, die mit einer Offenlegung der Nutzer verbunden ist, das Fernmeldegeheimnis gemäß § 88 TKG berührt, da nachvollziehbar ist, wer an dem Telekommunikationsvorgang beteiligt ist,[1125] so dass gemäß § 113 Abs. 1 S. 3 TKG die Voraussetzungen der einschlägigen gesetzlichen Vorschriften vorliegen müssen.[1126] So ist insbesondere ein richterlicher Beschluss gemäß §§ 100 g, h StPO erforderlich, so dass Strafverfolgungsbehörden nicht ohne weiteres die mit der Offenlegung der Benutzerauthentifizierungsdaten in gleichem Umfange offengelegten näheren Details der Kommunikation verlangen können. Ist also durch die Bekanntgabe der PIN-Nummern seitens der Strafverfolgungsbehörden ein unbeschränkter Zugriff auf die näheren Umstände der Kommunikation möglich, so ist dieser Zugriff nicht ohne Beteiligung eines Gerichts zulässig.

bbb. Inhalt der Telekommunikation

Sofern an einen von dem Provider betriebenen Gateway mehr als 1000 Kunden angeschlossen sind (für die er jeweils die Weiterleitung der Daten übernimmt), unterliegt der Provider gemäß § 3 TKÜV den Verpflichtungen der TKÜV,[1127] da er in diesem Falle eine Telekommunikationsdienstleistung für die Öffentlichkeit erbringt.

Zweifelhaft könnte allenfalls sein, wie § 3 Abs. 1 S. 2 TKÜV zu verstehen ist. Nach dieser Regelung, gilt die TKÜV nur für den Teil der Telekommunikationsanlage, die der Erbringung von

[1124] Siehe zur Eigenschaft des Providers als Telekommunikationsdienstanbieter S. 156 ff.

[1125] Zum Fernmeldegeheimnis siehe etwa Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 113; Groß in: Roßnagel, Handbuch Datenschutzrecht, 7.8 Rn. 8 (unter dieser Randnummer erfolgen Ausführungen bezüglich Eingriffen in das Fernmeldegeheimnis). Vgl. außerdem die Ausführungen auf S. 97 ff. in dieser Arbeit nebst weiteren Verweisen.

[1126] Siehe hierzu auch die Ausführungen in der Einführung S. 13.

[1127] Siehe auch § 3 Abs. 2 Nr. 5 TKÜV.

Telekommunikationsdiensten für die Öffentlichkeit dient. Werden mit einer Telekommunikationsanlage daher sowohl Telekommunikationsdienste für die Öffentlichkeit erbracht als auch andere Telekommunikationsdienste, ist der Provider in Bezug auf letztere von den Überwachungsmaßnahmen der TKÜV befreit. Denn hier könnte argumentiert werden, dass der Provider den Gateway zwar insgesamt einer Öffentlichkeit gemäß § 3 Nr. 19 TKG a.F. zur Verfügung stellt, aber dennoch im Hinblick auf jeden einzelnen Kunden einen individuellen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG erbringt.[1128]

Diese Frage soll hier nicht abschließend beantwortet werden. Sie betrifft vorrangig das Verhältnis zwischen dem Provider und einer Behörde und hat keine nachteiligere Auswirkung auf das datenschutzrechtliche Verhältnis zwischen Provider und VPN-Auftraggeber, da gemäß § 113 Abs. 1 S. 3 TKG ein Zugriff auf die Daten, die dem Fernmeldegeheimnis gemäß § 88 TKG unterliegen, nach den einschlägigen gesetzlichen Vorschriften und auf Anordnung ebenso erlaubt ist.[1129]

Die Anwendung der TKÜV ist vorrangig für den Provider aufgrund der von ihm zu tragenden Kostenlast und aufgrund der Vorhaltung der gesetzlichen Maßnahmen nachteilig.[1130] Der VPN-Auftraggeber ist aber datenschutzrechtlich nicht minder betroffen, sofern nicht TKÜV zur Anwendung gelangt, sondern im Einzelfall eine behördliche Anordnung, etwa nach §§ 100a, 100b Abs. 3 StPO, erfolgt.

Dies bedeutet, dass der Provider entweder gemäß § 5 Abs. 1, Abs. 2 TKÜV eine Kopie (des Inhalts) der Telekommunikation bereitstellen muss, oder aber gemäß § 100a StPO, § 100b Abs. 3 StPO, § 2 Abs. 1 Satz 3 des Artikel - 10 – Gesetzes, §§ 23a bis 23 c und 23e des Zollfahndungsdienstegesetzes oder nach Landesrecht zur Ermöglichung der Überwachung der Telekommunikation verpflichtet ist.[1131]

[1128] Siehe auch S. 260 ff., wo im Hinblick auf die Maßnahmen des § 109 Abs. 3 TKG ausgeführt worden ist, dass Benutzerauthentifizierung und Verschlüsselung des Gateway für jeden einzelnen VPN-Auftraggeber individuell gestaltet werden können.

[1129] Siehe hierzu auch die Ausführungen in der Einführung S. 13.

[1130] Siehe zur Kostenlast Groß in: Roßnagel, Handbuch Datenschutzrecht, 7.8 Rn. 22; Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 81. Vgl. außerdem die Ausführungen von Kloepfer in: Holznagel/Nelles/Sokol, TKÜV, S. 111 sowie Summa in: Holznagel/Nelles/Sokol, TKÜV, S. 29 ff.

[1131] Siehe zur Verpflichtung der Bereitstellung einer Kopie der Telekommunikation Bäumler in: Roßnagel, Handbuch Datenschutzrecht, 8.3 Rn. 57.

Im Hinblick auf die Überwachungsmaßnahmen ergeben sich jedoch Unterschiede zwischen Komplettmanagement des Gateways und Splitmanagement des Gateways, sofern der Provider bei letzterem die Funktionsherrschaft über den Gateway ausübt.[1132]

(1) Splitmanagement im Machtbereich des Providers

Übernimmt der Provider nur den Service des Gateways in seinem Machtbereich bzw. Räumlichkeiten, so erbringt er einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG bzw. wirkt gemäß § 3 Nr. 6b) TKG daran mit. [1133] Dementsprechend ist er gemäß § 113 TKG zur Auskunft verpflichtet oder nach § 3 TKÜV Verpflichteter der Überwachungsmaßnahmen, soweit der Gateway einer Vielzahl von Kunden zur Verfügung steht. Wird der Gateway nicht einer Allgemeinheit zur Verfügung gestellt, kann dennoch eine Verpflichtung zur Überwachung im Einzelfall bestehen. So bleiben gemäß § 3 Abs. 2 S. 3 TKÜV die Regelungen des § 100b Abs. 3 S. 1 StPO, § 2 Abs. 3 S. 1 des Artikel 10-Gesetzes, § 23a Abs. 8 des Zollfahndungsdienstegesetzes sowie die Vorschriften des Landesrechts zur Überwachung der Telekommunikation unberührt. Beispielsweise müsste der Provider im Falle des § 100 b Abs. 3 S. 1 StPO bei einer richterlichen Anordnung ebenso die Überwachung der Telekommunikationsinhalte ermöglichen. Allerdings ist der Provider in diesem Falle davon befreit, ständige Vorkehrungen für die Überwachungsmaßnahmen zu treffen bzw. vorzuhalten.[1134]

Bei dieser VPN-Variante (Splitmanagement im Machtbereich des Providers) ist es dem Provider jedoch nicht möglich, den berechtigten Stellen (etwa Strafverfolgungsbehörden) die unverschlüsselte Kommunikation bereitzustellen. Der Provider erbringt im Falle des Splitmanagement in seinem Machtbereich zwar insgesamt einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG, da die Verschlüsselungsprotokolle, wie IPSec oder L2Sec,[1135] lediglich die

[1132] Siehe zum Komplettmanagement das Bildbeispiel auf S. 49 und zum Splitmanagement das Bildbeispiel auf S. 52.
[1133] Siehe die Ausführungen auf S. 156 ff.
[1134] Vgl. auch S. 118 sowie Holznagel/Enaux/Nienhaus, Telekommunikationsrecht, Rahmenbedingungen – Regulierungspraxis, Rn. 708.
[1135] Zu Tunneling-Protokollen wie IPSec, L2Sec oder PPTP siehe S. 39 ff.

technische Basis des Datentransports darstellen. Die Verwendung der entsprechenden Protokolle ist in diesem Fall mit dem Telekommunikationsdienst verbunden bzw. ist diesem immanent.
Dennoch ist zu berücksichtigen, dass der Provider lediglich die verschlüsselte Kommunikation herausgeben kann, da er zum einen keinen Einfluss auf die Verschlüsselung seitens des VPN-Auftraggebers hat, und es zum anderen keine Verpflichtung zur Schlüsselhinterlegung gibt.[1136] Der VPN-Auftraggeber ist für die Sicherheitstechnik und die Benutzerverwaltung verantwortlich.[1137] Daher ist es dem Provider ebenso wenig möglich, Auskünfte über die Benutzerauthentifizierungen gemäß § 113 Abs. 1 S. 2 TKG i.V.m. §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO zu erteilen bzw. diese aufzuheben. Durch das Splitmanagement findet also eine funktionale Trennung der Verantwortungsbereiche auf dem Gateway statt.

(2) Komplettmanagement – Vergleichbarkeit mit GSM-Technik?

Im Falle des Komplettmanagements des Gateways durch den Provider, ist die Bereitstellung der Verschlüsselung auf dem Gateway sowie die Bereitstellung der Benutzerverwaltung durch den Provider abweichend von den gerade gemachten Ausführungen und den obigen Ausführungen zum Internetzugangsknoten zu betrachten.[1138] Es liegt gerade keine funktionale Trennung vor.
Der Provider ist hier als Telekommunikationsdienstanbieter dem VPN-Auftraggeber zur Bereitstellung der Verschlüsselungstechnik als Teil(leistung) des Telekommunikationsdienstes verpflichtet. Insbesondere ist es dem Provider auch möglich, die Verschlüsselung aufzuheben, da er diese (als Teil des von ihm gemäß § 3 Nr. 24 TKG erbrachten Telekommunikationsdienstes) selbst erzeugt hat und diese unmittelbar mit dem Telekommunikationsvorgang zusammenhängt.[1139]

[1136] Vgl. Schaar in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 402 zur Hinterlegungspflicht von verwendeten Schlüsseln sowie außerdem Fn. 1026 in dieser Arbeit.
[1137] Siehe zum Splitmanagement das Bildbeispiel auf S. 52.
[1138] Siehe die Ausführungen auf S. 238 ff.
[1139] Siehe auch Rieß, DuD 1996, 328, 331, der erwähnt, dass nur solche Befugnisnormen eine Durchbrechung des Fernmeldegeheimnisses rechtfertigen, die sich ausdrücklich auf Telekommunikationsvorgänge beziehen. Da auch hier die Verschlüsselung mit einem Telekommunikationsvorgang verbunden ist, ist eine zulässige Durchbrechung anzunehmen.

Da § § 3 TKÜV sowie § 100b Abs. 3 StPO, des § 2 Abs. 1 Satz 3 des G-10-Gesetzes, §§ 23a bis 23 c und 23e des Zollfahndungsdienstegesetzes oder Landesrecht insgesamt den Anbieter eines Telekommunikationsdienstes zur Aufzeichnung bzw. zur Ermöglichung der Aufzeichnung von Telekommunikation auf Anordnung verpflichten, ist damit auch zwangsläufig die Aufhebung der entsprechenden Verschlüsselung verbunden. In diesem Falle ist die Aufhebung der Verschlüsselung für den Provider ebenso realisierbar, da die Schlüsselerzeugung beim Komplettmanagement technischer Bestandteil des von dem Provider erbrachten Telekommunikationsdienstes ist.

Es liegt hier eine Vergleichbarkeit mit einer netzseitigen Verschlüsselung vor, die bislang nur für die GSM-Techniken bejaht werden konnte.[1140] Auch bei GSM wird gemäß § 8 Abs. 3 TKÜV eine Aufhebung der Verschlüsselung verlangt.[1141] Die Vergleichbarkeit ist insbesondere deswegen folgerichtig, da in beiden Fällen auf eine „Basisstation", die beim VPN der Gateway darstellt, zugegriffen wird, die für die Verschlüsselung verantwortlich ist.[1142]
Daher kann eine netzseitige Verschlüsselung nicht nur für Mobilfunknetze,[1143] sondern ebenso für ein VPN in Betracht kommen, sofern der Provider das Komplettmanagement übernimmt.

Vgl. außerdem Baum/Trafkowski, CR 2002, 69, 70 ff. sowie zu § 8 Abs. 3 TKÜV auch Pernice, DuD 2002, 207, 209 und Hamm in: Holznagel/Nelles/Sokol, TKÜV, S. 88.

[1140] Siehe zum GSM-Standard S. 196, insbesondere Fn. 840 Siehe außerdem Beheim, DuD 1994, 327 ff. sowie die Ausführungen des Bundesbeauftragten für den Datenschutz „Begründung zum Entwurf einer Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV), abrufbar unter www.bfd.bund.de/information/symp2_ulrich3.html (Website vom 01.08.2004).

[1141] Siehe die Ausführungen des Bundesbeauftragten für den Datenschutz „Begründung zum Entwurf einer Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV), abrufbar unter www.bfd.bund.de/information/symp2_ulrich3.html (Website vom 01.08.2004)

[1142] Beheim, DuD 1994, 327, 330 legt dar, dass die Verschlüsselung auf der Funkstrecke zwischen Mobilgerät und einer Basisstation des Anbieters (die auf „der anderen Seite" für die Verschlüsselung verantwortlich ist). Auch ein Gateway ist für die Verschlüsselung „als Basisstation" verantwortlich (siehe zur Funktion eines Gateways ebenso S. 46 sowie das Angebot von T-Online „Secure-VPN-Benutzerhandbuch", S. 216, wo unter anderem darauf verwiesen wird, dass auf dem Gateway die Entschlüsselung der Daten stattfindet.

[1143] In seiner Begründung zu § 8 TKÜV legt der Bundesbeauftragte für den Datenschutz dar (siehe den Fundstellennachweis in Fn. 1141), dass die netzseitige Bereitstellung von Verschlüsselung nach dem heutigen Stand der Technik nur für Mobilfunknetze nach dem GSM-Standard möglich ist.

Zwar kann darüber hinaus der Gedanke nahe liegen, dass die Funktion der Datenverschlüsselung eines Tunneling-Protokolls über das, was für die eigentliche Nachrichtenübermittlung erforderlich ist, hinausgeht, so dass nicht mehr der eigentliche Datentransport im Vordergrund steht, und damit ein Dienst zur Nutzung des Internets gemäß § 2 Abs. 2 Nr. 3 TDG in Betracht kommen könnte.[1144] So bieten insbesondere Protokolle wie IPSec oder L2Sec neben der Verschlüsselung des Dateninhalts die Möglichkeit, einen neuen IP-Header an das Datenpaket zu fügen, was aber für den Transport des ursprünglichen Datenpaketes nicht notwendig ist.[1145]
Nichtsdestotrotz ist eine Einstufung der Verschlüsselungstechnik als Teledienst insgesamt nicht folgerichtig. Denn zu beachten ist, dass die Verschlüsselung(stechnik) an sich keinen Inhalt darstellt, und unter Telediensten lediglich Angebote verstanden werden, auf die ein Nutzer in bewusster Weise zugreifen kann und die dem Nutzer verschiedene Informationen liefern.[1146]

Auch bei den Tunneling-Protokollen mit Verschlüsselungstechnik handelt es sich daher um Internet-Dienste.[1147] Tunneling-Protokolle sind also „lediglich“ technische Möglichkeiten, die den Datenaustausch im Internet ermöglichen,

[1144] In diesem Falle könnte damit ein Teledienst im Sinne von § 2 Abs. 2 Nr. 3 TDG (Dienst zur Nutzung des Internet) vorliegen.
[1145] Der Nutzer (Client) muss, um die Verschlüsselung im Rahmen des Tunnels einsetzen zu können, auf den Gateway (Server) an einem anderen Standort bzw. auf spezielle VPN-Software zugreifen.
Im Rahmen von IPSec wird außerdem der Schlüssel über das Internet, also von einem Netzwerk bzw. Rechner zu dem zu kontaktierenden Netzwerk bzw. Rechner, übertragen (Die Übertragung dieses einen Schlüssels im Rahmen von IPSec über das Internet, also von einem Netzwerk bzw. Rechner zu dem zu kontaktierenden Netzwerk bzw. Rechner, erfolgt asymmetrisch, vgl. auch S. 41 ff. sowie Lipp, VPN, S. 94). Streng genommen geht es bei IPSec nicht vordergründig darum, überhaupt Daten zu übertragen, sondern darum, diese sicher zu übertragen und das Internet sicher zu nutzen. IPSec wurde aufgrund zunehmender Kommerzialisierung des Internets und Änderung von dessen Sicherheitsanforderungen entwickelt, um hochwertige, auf Kryptographie basierende Sicherheit für IP-Datenübermittlung zu bieten (Davis, IPSec, S. 192). Entsprechendes gilt auch für das Protokoll L2Sec. Anders als bei L2TP sollen mittels IPSec und L2TP nicht nur allein Daten über das Internet transportiert werden, sondern diese Daten hauptsächlich auch sicher vor Zugriffen von außen übermittelt werden. Hierzu gehört bei IPSec und L2Sec unter anderem die Möglichkeit, die Absender zu verstecken, in dem ein neuer Header an das Datenpaket gefügt wird. Die reine Datenübertragung würde jedoch nicht erfordern, den Header durch einen neuen zu ersetzen.
[1146] Siehe oben S. 129 ff. und insbesondere Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 87 Fn. 459, der Access-Provider als Telediensteanbieter dann ablehnt, sofern diese keine eigenen Angebote auf einer Website bereitstellen.
[1147] Zu den Internet-Diensten siehe die Ausführungen auf S. 75 ff nebst Verweisen.

ohne selbst aber Telekommunikationsdienste gemäß § 3 Nr. 24 TKG oder Teledienste gemäß § 2 Abs. 1 TDG darzustellen.

Hier kann zudem die berechtigte Frage gestellt werden, wie die Pflichten des Providers, über die Netzsicherheit aufzuklären und für die Betriebssicherheit gemäß § 109 TKG unter Berücksichtigung von Artikel 4 der EU-Richtlinie 2002/58/EG mit den Überwachungsmaßnahmen in Einklang zu bringen sind. Denn der Provider müsste gegebenenfalls dem VPN-Auftraggeber raten, das Management des Gateways und die Verschlüsselung der Daten selbst zu übernehmen. Insoweit besteht daher ein Widerspruch.

Generell ist es rechtlich jedoch nicht zu beanstanden und stellt für den Provider keine unzumutbare Benachteiligung dar, sofern er beispielsweise in seinen Produktbeschreibungen oder Datenschutzhinweisen darüber informiert, dass er im Falle des Komplettmanagement zu Überwachungsmaßnahmen verpflichtet ist. Es wäre lediglich nicht erlaubt, den Kunden im Einzelfall darüber zu informieren, dass dieser überwacht wird, wobei dies für das manuelle Auskunftsverfahren in §§ 113 Abs. 1 S. 4, 149 Abs. 1 Nr. 35 TKG geregelt ist und eine Ordnungswidrigkeit darstellt.

4. Zusatzdienst E-Mail

Beim Zusatzdienst E-Mail sind im Hinblick auf die Datenschutz- und Datensicherheitsmaßnahmen entsprechend des im zweiten Abschnitt dieser Arbeit dargestellten Prüfungsschemas wiederum die Fragestellungen der Datenvermeidung, der technischen Schutzmaßnahmen auf den E-Mail-Systemen sowie die Problematik der Schranken des Datenschutzes aufgrund von gesetzlichen Überwachungsmaßnahmen und Auskunftsverpflichtungen zu prüfen.[1148]

Dementsprechend muss zunächst dargestellt werden, welche Daten grundsätzlich beim E-Mail-Dienst anfallen.

a. Datenvermeidung

aa. Verkehrsdaten

Der Provider erstellt auf seinen Mailservern[1149] Log-Files,[1150] die sich auf die näheren Umstände des Zugriffs durch den Nutzer, wie Datum, Uhrzeit, Benutzername, etc. beziehen.

Sofern der Access-Provider als Zusatzdienst dem VPN-Auftraggeber bzw. dessen Nutzern E-Mail-Accounts und Mailserver bereitstellt,[1151] ist fraglich, inwieweit die E-Mail-Adresse sowie die sonstigen Daten der Verbindung, wie Datum, Uhrzeit, Datenvolumen, gemäß §§ 96 ff. TKG[1152] zu löschen sind. Bei einer juristischen Person gilt, dass dem Fernmeldegeheimnis unterfallende Daten gemäß § 91 Abs. 1 S. 2 TKG den personenbezogenen Daten gleichstehen, also insbesondere die Frage, wer zu welchem Zeitpunkt kommuniziert hat.[1153]

Regelmäßig richtet der VPN-Auftraggeber seinen Mitarbeitern E-Mail-Accounts ein, so dass diese eine eigenständige E-Mail-Kommunikation mit Dritten führen

[1148] Siehe die Darstellung der datenschutzrechtlichen Pflichten auf S. 106 ff. sowie S. 162 ff. Siehe außerdem den Hinweis auf S. 121.
[1149] Siehe hierzu das Bildbeispiel in der Einführung S. 63.
[1150] Vgl. zu Log-Files S. 178.
[1151] Siehe hierzu S. 3.
[1152] Siehe S. 157 ff. und der Einordnung als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG.
[1153] Siehe zur Definition des Fernmeldegeheimnisses S. 97.

können. Da die E-Mail-Adressen der Nutzer des VPN-Auftraggebers meist dessen Unternehmensnamen bzw. Firma als Domain-Namen enthalten, wie etwa Nutzer-YX@Unternehmen-XY.de, ist die Speicherung dieser Absender-Adresse und der jeweiligen Ziel-Adresse nebst Datum und Uhrzeit ein Umstand, der den VPN-Auftraggeber in seinem Fernmeldegeheimnis gemäß § 88 TKG betrifft.[1154] Denn es wäre nachvollziehbar, zu welchem Ziel vom VPN-Auftraggeber aus eine Kommunikationsverbindung aufgebaut worden ist.

Fraglich ist allerdings, ob dies auch gilt, sofern der VPN-Auftraggeber seinen Nutzern bzw. Mitarbeitern ebenso die private Internetnutzung erlaubt. Denn dann wäre er nicht unter allen Umständen mit der E-Mail-Kommunikation in Verbindung zu bringen bzw. würde es sich nicht um „seine" Kommunikation handeln.

Daher könnte problematisch sein, ob der Access-Provider im Verhältnis zum VPN-Auftraggeber überhaupt zur Löschung der Verkehrsdaten nach § 96 Abs. 2 TKG verpflichtet ist, wenn der VPN-Auftraggeber seinen Nutzern, wie etwa Mitarbeitern, die Nutzung des E-Mail-Dienstes nicht allein und ausschließlich zu beruflichen Zwecken erlaubt.[1155]
Zu berücksichtigen ist aber in diesem Zusammenhang, dass dies einen internen bzw. innerbetrieblichen Vorgang darstellt, den der Provider in der Regel nicht kennt. Sofern der Provider also auf seinen Systemen nicht unterteilen kann, welche E-Mails privat und welche geschäftlich sind, so muss er insgesamt die

[1154] Hieran zeigt sich ebenso, dass die Einordnung der entsprechenden Dienste in Telekommunikationsdienste oder Teledienste von großer Relevanz ist, da das TDDSG keine Regelungen bezüglich des Fernmeldegeheimnisses enthält, und dieses daher nur dann zu berücksichtigen ist, sofern es sich um einen Telekommunikationsdienst handelt.

[1155] Siehe zur privaten Nutzung des Internet und E-Mails aber auch Rosen, The unwanted gaze, The destruction of privacy in America, S. 54 ff. und 159 ff. Aus seinen Ausführungen kann der Schluss gezogen werden, dass die private Nutzung des Internets alltägliches Kommunikationsverhalten der Arbeitnehmer geworden ist. So berichtet er auf S. 161/162 von einem anonymen Artikel eines Technikers in dem Online-Magazin „Salon", in welchem dieser darauf hinweist, dass er während seiner Beschäftigung an der Harvard Divinity School mittels eines Programms namens „Gatekeeper" die Möglichkeit hatte, die in der Schule geführte Kommunikation bis zu einem einzelnen Endnutzer zu rekonstruieren und dabei feststellte, dass sehr oft zu privaten Zwecken kommuniziert worden ist. Auf S. 89 weist Rosen darauf hin, dass in einigen Studien die private E-Mail-Kommunikation auf 40% geschätzt wird. Siehe ebenso Rosen, S. 76: „On any company network, a user´s e-mail folders of sent and received messages are likely to contain a range of public and private expression, from the official statements of company policy that are traditionally found in letters to the private jokes and flirtation that used to take place around the watercooler". Außerdem Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 124 mit dem Hinweis, dass die elektronische Post beim Einsatz in einem Unternehmen oftmals die Kommunikation per Telefon ersetzt.

Löschung von Absender- und Zieladresse, Datum und Uhrzeit gemäß § 96 Abs. 2 TKG sowohl auf seinem SMTP-Server als auch PoP3-Server vornehmen, da er ansonsten gegen seine gesetzlichen Löschungspflichten gegenüber dem VPN-Auftraggeber verstoßen würde.[1156]

Diese Pflicht beruht auf einer Gefährdung des Fernmeldegeheimnisses des VPN-Auftraggebers, ohne dass im Einzelfall eine tatsächliche Verletzung des Fernmeldegeheimnisses nach § 88 TKG vorliegen muss.[1157]

Zum Zwecke der Klarstellung soll hier nochmals betont werden, dass sich die obigen Ausführungen lediglich auf das Verhältnis zwischen Provider und VPN-Auftraggeber beziehen. Dies bedeutet, dass die Auswirkungen auf die Interessen des Nutzers erst im Verhältnis zwischen Provider und Nutzer sowie VPN-Auftraggeber und Nutzer zu prüfen sind.[1158]

Festzuhalten ist aber, dass sich allein aus den Regelungen des TKG im Verhältnis zwischen VPN-Auftraggeber und Provider keine unmittelbare Verpflichtung gegenüber dem Nutzer ergibt, die Verkehrsdaten des Nutzers zu löschen.

Eine solche Pflicht kann sich erst aus einer Gesamtschau der Beteiligtenverhältnisse ergeben, etwa wenn festgestellt wird, dass der Provider auch gegenüber dem Nutzer datenschutzrechtliche Pflichten zu wahren hat.

Im Verhältnis zwischen VPN-Auftraggeber und Provider interessiert aber allein die Fragestellung, ob der Provider gegenüber dem VPN-Auftraggeber „weniger“ datenschutzrechtliche Pflichten hat, wenn die jeweiligen Nutzer, wie etwa die Mitarbeiter des VPN-Auftraggebers, privat kommunizieren.

[1156] Dies gilt ebenso für andere Verkehrsdaten im Sinne von § 96 Abs. 2 TKG, soweit solche anfallen.

[1157] Vgl. Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 27 zur „Ausstrahlung“ des Fernmeldegeheimnisses auf die geschäftliche Kommunikation und zum Erfordernis der Trennung der Telekommunikationsanlagen im Rahmen der betrieblichen Kommunikation. Entsprechendes muss auch im Verhältnis zwischen Provider und VPN-Auftraggeber gelten, sofern eine Trennung der Systeme nicht möglich ist. Siehe auch Däubler in: Ahrens/Donner/Simon, Arbeit-Umwelt, 2001, S. 1, 6, der allerdings das Verhältnis zwischen Arbeitgeber und Arbeitnehmer untersucht, aber dennoch klargestellt, dass Daten zu löschen sind, sofern die Systeme nicht in der Lage sind, die private Nutzung von der dienstlichen Nutzung zu trennen.

[1158] Siehe zu der Frage, inwieweit ein Provider gegenüber dem Nutzer eines E-Mail-Dienstes (mit dem er keinen Vertrag geschlossen hat) verpflichtet ist, die nachfolgenden Ausführungen auf S. 294 ff.

bb. Inhaltsdaten

Wie sich aus dem Wortlaut des § 88 Abs. 1 TKG ergibt, fällt der Inhalt der E-Mail unter das Fernmeldegeheimnis.
Die E-Mail(-Datei) besteht aus dem Nachrichtenteil, der als Hauptteil den Inhalt bzw. Text der E-Mail und als weiteren Teil den so genannten Header enthält, der aus Zieladresse, Datum, Uhrzeit und Betreffzeile besteht.[1159] Ein zweiter Bestandteil ist die Absenderadresse, die mit einem Umschlag bei der Briefpost vergleichbar ist.[1160] Inhalt, Header und Absenderadresse sind also in einer Datei miteinander verknüpft, und dürfen daher gemäß § 96 Abs. 2 TKG insgesamt nur für den Zeitraum gespeichert werden, der für die Übertragung und den Abruf der E-Mail notwendig ist, wenn hier eine untrennbare Verknüpfung vorliegt.[1161] Diesbezüglich ergeben sich Unterschiede in Abhängigkeit des verwendeten E-Mail-Protokolls, die nachfolgend dargestellt werden.[1162]

Bei Verwendung des POP3-Protokolls ist für den POP3-Server eine längere Speicherungsfrist erforderlich, da der Abruf und damit die Übertragung der E-Mail vom Nutzer abhängt und länger andauern kann. Nach Abruf der E-Mail durch den Nutzer bzw. VPN-Auftraggeber ist dennoch keine längerfristige Speicherung erforderlich, da sich nunmehr die E-Mail auf dem Rechner des Nutzers bzw. VPN-Auftraggebers befindet, so dass eine automatische Löschung der E-Mail-Datei auf dem POP3-Server stattfinden kann.[1163]
Da es im Übrigen keine Mindestspeicherungsfristen gibt, wäre es für den Provider eines E-Mail-Dienstes ebenso möglich, den VPN-Auftraggeber bzw. seinen Kunden darauf hinzuweisen, dass er E-Mails beispielsweise lediglich für einen Zeitraum von vier Wochen zum Abruf auf seinem POP3-Server vorhält.

[1159] Vgl. Tanenbaum, Computernetzwerke, S. 644.
[1160] Vgl. Voss, Das große PC & Internet Lexikon 2007, S. 411, der unter dem Begriff des Headers aber ebenso die Absenderadresse erfasst.
[1161] Vgl. auch Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 122.
[1162] Siehe zu den Protokollen der E-Mail-Kommunikation S. 62 ff.
[1163] Siehe Tanenbaum, Computernetzwerke, S. 659 mit dem Hinweis, dass nach Herunterladen der E-Mail auf den Rechner des Nutzers sich die einzige Kopie der E-Mail auf dem Rechner des Nutzers befindet.

Sofern der Provider das Protokoll IMAP[1164] einsetzt, ist er seinem Kunden bzw. dem VPN-Auftraggeber gegenüber vertraglich verpflichtet, sämtliche E-Mails (stets unter Wahrung des Fernmeldegeheimnisses gemäß § 88 Abs. 1 TKG) auf seinem Server mindestens bis zum Vertragsende zu speichern, da diese langfristige Speicherung gerade Sinn und Zweck des unter Verwendung von IMAP geschlossenen Vertragsverhältnisses ist.
Der Provider ist damit erst bei Vertragsende gemäß § 96 Abs. 2 TKG zur unverzüglichen Löschung der Daten verpflichtet, soweit diese nicht mehr für Abrechnungszwecke gemäß § 97 TKG oder für die weiteren in §§ 99 und 100 TKG genannten Zwecke erforderlich sind. Zu berücksichtigen ist dennoch, dass einer unverzüglichen Löschung gegebenenfalls zivilvertragliche Aufbewahrungspflichten entgegenstehen können.

Die Verwendung des SMTP-Protokolls hat zur Folge, dass der Provider des SMTP-Servers zur Löschung des Nachrichtenteils sowie der Absenderadresse unmittelbar nach Weiterleitung der E-Mail verpflichtet ist, soweit sich aus §§ 97, 99 und 100 TKG nichts anderes ergibt.[1165] Der Nachrichtenteil bzw. die inhaltlichen Daten der E-Mail sind zwar nicht in der abschließenden Liste des § 96 Abs. 1 TKG als Verkehrsdaten erwähnt.[1166] Die oben dargestellte Struktur der E-Mail (Inhalt, Header und Absenderadresse sind in einer Datei miteinander verknüpft) führt jedoch dazu, bei Löschung der Absenderadresse die Löschung des Inhalts zwangsläufig mit erfasst ist.
Im Rahmen der Verwendung von SMTP ist darüber hinaus zu berücksichtigen, dass die E-Mail-Adresse des VPN-Auftraggebers auf dem SMTP-Server zum Zwecke der Authentifizierung gespeichert werden muss.[1167] In diesem Falle stellt die E-Mail-Adresse ein für den Aufbau weiterer Verbindungen gemäß § 96 Abs. 2 TKG notwendiges Datum dar und ist als Verkehrsdatum gemäß § 3 Nr. 30 TKG einzuordnen. Der Personenbezug liegt vor, da der Kunde bzw. VPN-

[1164] Siehe zu dem Protokoll IMAP S. 62.
[1165] Siehe hierzu ebenso das Bildbeispiel auf S. 63.
[1166] Vgl. Büchner in: TKG-Kommentar, § 5 TDSV (Anh § 89 TKG) Rn. 1; Robert in: TKG-Kommentar (3. Auflage), § 96 TKG Rn 2. Vgl. zur abschließenden Festlegung zulässiger Zwecke im TKG auch Gramlich in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 89 TKG(1998), Band 1, Rn. 45.
[1167] Siehe zur Authentifizierung auf dem SMTP-Server auch Voss, Das große PC & Internet Lexikon 2007, „SMTP“ S. 740 ff.

Auftraggeber dem Provider als dessen Vertragspartner bekannt ist und damit die Bestimmbarkeit gegeben ist.[1168]

Dies bedeutet, dass der Provider, der den E-Mail-Account bereitstellt, die E-Mail-Adresse seines Kunden für die Vertragslaufzeit auf dem SMTP-Server für Zwecke des Verbindungsaufbaus separat speichern muss und auch darf, aber die gesamte E-Mail oder Logdateien gemäß § 96 Abs. 2 TKG unverzüglich löschen muss, soweit diese nicht mehr benötigt werden.
Dementsprechend ist der Provider bei Beendigung des mit dem VPN-Auftraggeber eingegangenen Vertragsverhältnisses zur Löschung der E-Mail-Adresse verpflichtet, da er diese nicht mehr für den Aufbau weiterer Verbindungen benötigt. Etwas anderes ergibt sich allenfalls dann, sofern der Provider die E-Mail-Adresse für die Zwecke der §§ 97, 99 und 100 TKG, insbesondere zur Entgeltabrechnung gemäß § 97 TKG, über das Ende des Vertragsverhältnisses hinaus benötigen würde.

Würde hingegen die E-Mail-Adresse als Bestandsdatum[1169] eingestuft werden, wäre der Provider gemäß § 95 Abs. 3 TKG berechtigt, die E-Mail-Adresse bis zum Ablauf des auf die Beendigung folgenden Kalenderjahres zu speichern. Die Speicherdauer würde sich damit erheblich verlängern. Allerdings ist die pauschale Einordnung der E-Mail-Adresse als Bestandsdatum nicht folgerichtig. Vielmehr ist wiederum auf die Verwendung im Einzelfall abzustellen. Auch in diesem Zusammenhang muss gelten, dass die E-Mail-Adresse kein Bestandsdatum im Sinne von § 3 Nr. 3 TKG darstellen kann, da dieses Datum seitens des Providers nicht erhoben, sondern „erschaffen“ worden ist.[1170] Im Verhältnis zu Dritten, mit denen der Kunde ein Vertragsverhältnis eingeht und hierbei seine E-Mail-Adresse angeben muss, kommt hingegen ein Bestandsdatum gemäß § 3 Nr. 3 TKG in Betracht. [1171] Entsprechendes gilt, sofern der Provider die E-Mail-Adresse des VPN-Auftraggebers darüber hinaus bzw. zusätzlich im Rahmen des VPN-Vertrages oder E-Mail-Dienstvertrages für

[1168] Siehe zur Bestimmbarkeit S. 94.
[1169] Vgl. zur Einstufung der E-Mail-Adresse als Bestandsdatum Dix in: Roßnagel, Recht der Multimedia-Dienste, § 5 TDDSG Rn. 33.
[1170] Siehe S. 168. Vgl. auch Schneider, Verträge über Internet-Access, S. 212, die darlegt, dass dem Nutzer seitens des Providers eine E-Mail-Adresse zugewiesen wird.
[1171] Siehe hierzu auch die Ausführungen in Fn. 738.

die Erfüllung eigener (weiterer) vertraglicher Leistungen benötigen würde. Hier kommt beispielsweise die Speicherung der E-Mail-Adresse zum Zwecke der Rechnungsstellung oder Mitteilung vertragswesentlicher Informationen in Betracht. In diesen Fällen handelt es sich bei der E-Mail-Adresse (auch) um ein Grunddatum des Vertrages gemäß § 3 Nr. 3 TKG, welches jedoch auf einem anderem System bzw. Datenträger, z.B. einem Arbeitsrechner, gespeichert wird.

Daher zeigt sich wiederum, dass die konkrete Datenverarbeitung auf dem jeweiligen technischen System entscheidend ist, da die E-Mail-Adresse sowohl Bestandsdatum als auch Verkehrsdatum sein kann, je nachdem welches Personenverhältnis oder Kontext zugrunde gelegt wird.

Dies ist wichtig, da unterschiedliche Löschungsfristen für unterschiedliche Systeme in Betracht kommen können.

b. Technische Schutzmaßnahmen

aa. Unterrichtungspflichten über Netzsicherheit

Derjenige Provider, der dem VPN-Auftraggeber den E-Mail-Service bereitstellt und Betreiber des SMTP-Servers ist, ist ebenso gemäß § 109 Abs. 1 TKG zur Aufklärung über die Verschlüsselungstechniken verpflichtet.[1172]

Hier gelten die Ausführungen zum Thema „Unterrichtungspflichten beim Access-Providing“ entsprechend,[1173] so dass dem Provider insgesamt zumutbar ist, auf entsprechende Maßnahmen, beispielsweise auf seiner Website hinzuweisen.

Bei E-Mails kommt vor allem das Programm „Open Pretty Good Privacy“ (OpenPGP) sowie die Alternativsoftware GNUPG und GNUPP in Betracht, die seit Anfang 2002 vom Bundesamt für Sicherheit in der Informationstechnik

[1172] Siehe auch die Ausführungen von Koenig/Röder, CR 2000, 668, 671/672, die im Hinblick auf die Verschlüsselungsverpflichtung eines Anbieters darstellen, dass diese nur durch den Stand der Technik eingeschränkt wird, so dass bei E-Mails anders als bei der Übertragung von Daten im Rahmen von WWW-Angeboten keine entsprechende Verpflichtung zur Verschlüsselung besteht (dies galt zumindest zum damaligen Zeitpunkt). Zu berücksichtigen ist bei dieser Ansicht wie gesagt, dass die Regelungen der EU-Richtlinie 2002/58/EG allein für die Anbieter von Telekommunikationsdiensten gelten (S. 8 Fn. 29), so dass hier gleichermaßen eine entsprechende Unterrichtungspflicht für den Provider eines E-Mail-Dienstes gelten muss, da insoweit kein Unterschied zur Bereitstellung eines Internetzugangs besteht (vgl. die Ausführungen auf S. 234 ff.).

[1173] Siehe oben S. 196. Siehe aber auch die Ausführungen auf S. 234 ff.

empfohlen wird.[1174] Der Provider kann insbesondere auch hier die Verschlüsselungen im Sinne von § 109 Abs. 1 TKG nicht selbst vornehmen, da dies eine technische Voraussetzung ist, die lediglich von dem Teilnehmer bzw. vom VPN-Auftraggeber durchgeführt werden kann.[1175]
Zu bedenken ist allerdings, inwieweit PGP oder GNUPP und GNUPG aufgrund ihres Open Source Status ohnehin bereits allgemein bekannt sein könnten, so dass sich eine solche Unterrichtungspflicht erübrigen könnte. Nichtsdestotrotz sollte der Provider beispielsweise auf seiner Website einen Link auf PGP-Freewareversion oder GNUPG sowie GNUPP setzen und den Kunden beim Abschluss des Vertrages über E-Mail-Dienste über die Möglichkeiten einer sicheren Kommunikation unterrichten.

Die Alternativsoftware GNUPG sowie GNUPP haben im Gegensatz zu PGP den Vorteil, dass es sich um eine Opensource-Software handelt, während PGP lediglich für den privaten Gebrauch als Freeware erhältlich ist. Als Opensource-Software ist insgesamt der Quelltext von GNUPG einsehbar, und der jeweilige Nutzer kann dieses Programm an seine Bedürfnisse anpassen.[1176]

bb. Anforderungen an Mailserver

Der Provider ist gemäß § 109 Abs. 2 TKG verpflichtet, für die Sicherheit der Mailserver[1177] Sorge zu tragen. Bei Mailservern, die die Weiterleitung der E-Mails übernehmen, handelt es sich um Telekommunikationsanlagen gemäß § 3 Nr. 23 TKG, da sie als technische Einrichtungen oder Systeme als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Systeme sind einzelne oder mehrere Geräte, deren Bestandteile in ihrer Gesamtheit die

[1174] Siehe hierzu Voss, Das große PC & Internet Lexikon 2004, S. 655 ff (in der aktuellen Auflage „2007“ finden sich keine Hinweise zu GNUPP). Siehe für nähere Informationen zu GNUPG und GNUPP http://www.Gnupg.org und http://www.gnupp.de. Siehe zu PGP Däubler, Internet und Arbeitsrecht, Rn. 44
[1175] Vgl. Schaar in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 401 und der Ausführung, dass der Schlüsselaustausch zwischen den Kommunikationspartnern stattfindet. Insoweit ist die Aussage, dass kaum E-Mail-Anbieter Verschlüsselungen anbieten, so dass sich der Kunde selbst darum kümmern muss (Koenig/Röder, CR 2000, 688, 672), etwas missverständlich. Denn es obliegt stets dem Kunden, entsprechende Verschlüsselungsmechanismen einzusetzen.
[1176] Siehe hierzu Voss, Das große PC & Internet Lexikon 2004, S. 655 (in der aktuellen Auflage 2007 sind keine Hinweise zu GNUPP enthalten).
[1177] Siehe hierzu, insbesondere zu diesem Begriff das Bildbeispiel auf S. 63.

Aufgabe der Telekommunikations- bzw. sonstigen Datenverarbeitung ermöglichen.[1178] Für die Verpflichteten nach § 109 Abs. 2 TKG sind Telekommunikationsanlagen ebenfalls zugleich als Telekommunikationssysteme zu betrachten.[1179]

Wie dargestellt,[1180] stellen Mailserver die notwendigen technischen Voraussetzungen dar, um die E-Mail-Kommunikation überhaupt erst ermöglichen zu können. Sie stehen außerdem einer Öffentlichkeit zur Verfügung, da auf sie eine Vielzahl nicht abgrenzbarer oder mittels eines gemeinsamen Zwecks verbundener Personen im Rahmen des E-Mail-Dienstes zugreift.[1181]
Auch hier muss daher seitens des Providers ein Sicherheitskonzept gemäß § 109 Abs. 3 TKG erarbeitet werden.[1182]

c. Auskunfts- und Überwachungspflichten

Von besonderer Bedeutung ist in diesem Zusammenhang, dass der Provider gemäß § 113 Abs. 1 TKG unverzüglich Auskünfte über die nach den §§ 95 und 111 TKG erhobenen Daten zu erteilen hat, und darüber hinaus ebenso zum Kreis der Verpflichteten nach § 3 TKÜV gehört.[1183]

[1178] Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 28.
[1179] Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 28.
[1180] Siehe S. 157 ff.
[1181] Vgl. hierzu etwa Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 100. Siehe insbesondere zu den Voraussetzungen eines Telekommunikationsdienstes für die Öffentlichkeit S. 116 ff.
[1182] Siehe zu den Anforderungen eines Sicherheitskonzeptes S. 114 unter Verweis auf Zimmer, CR 2003, 896, 898. Siehe außerdem Heibey in: Roßnagel, Handbuch Datenschutzrecht, 4.5 Rn. 30.
[1183] Siehe S. 238 ff. Vgl. außerdem Ullrich in: Holznagel/Nelles/Sokol, TKÜV, S. 20, der ebenso der Meinung ist, dass E-Mails zweifelsfrei unter den Begriff der Telekommunikation zu fassen sind. Dementsprechend ist deren Überwachung durch die Vorschriften der StPO, des G-10-Gesetzes und des AWG (nun Zollfahndungsdienstegesetz) abgedeckt. Ullrich (aaO) weist ebenso darauf hin, dass es mittlerweile bereits eine ganze Reihe von rechtmäßig ergangenen Überwachungsanordnungen im Hinblick auf E-Mails gibt. Siehe außerdem die Ausführungen der Bundesnetzagentur, abrufbar unter http://www.bundesnetzagentur.de/enid/78f203c9cbedb13a969685e262e885f3,55a304092d09/Technische_Umsetzung_von_Ueberwachungsma_nahmen/Zusaetzliche_Informationen_fuer_die_Betreiber_von_E-_np.htmlhttp://www.regtp.de/tech_reg_tele/03009/index.html (Website vom 30.09.2006) sowie die dort abrufbaren technischen Einzelheiten der Überwachungstechnik für E-Mail-Server der Technischen Richtlinie zur Beschreibung der Anforderungen an die Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜ), Ausgabe 4.1 vom 29.11.2004 (unter http://www.bundesnetzagentur.de/media/archive/2587.pdf - Website vom 30.09.2006). Siehe zur TR TKÜ ebenso Bock in: TKG-Kommentar (3. Auflage), § 110 TKG Rn. 90.

Nach § 5 TKÜV ist der Provider zur Umsetzung einer Überwachungsmaßnahme verpflichtet sind und muss der berechtigten Stelle[1184] am Übergabepunkt eine vollständige Kopie der Telekommunikation bereitstellen müssen, die über seine Telekommunikationsanlage abgewickelt wird.
Dies bedeutet aber, dass er im Falle der Verschlüsselung von E-Mails nur eine verschlüsselte Kommunikation bereitstellen kann.
Selbst wenn der Provider technisch dazu in der Lage ist, ist er nicht verpflichtet, die seitens eines Teilnehmers vorgenommene Verschlüsselung aufzuheben.
Nach § 8 Abs. 3 TKÜV muss ein Provider lediglich netzseitige Verschlüsselungen aufheben, so dass insoweit auf die obigen Ausführungen verwiesen wird.[1185]

Ergänzend sei hier darauf hingewiesen, dass sich anhand dieses Themas im Besonderen die praktische Relevanz der Einordnung eines Dienstes als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG oder Teledienst gemäß § 2 Abs. 1 TDG zeigt. Der Provider würde bei Einordnung eines E-Mail-Dienstes als Teledienst den Überwachungspflichten von vorneherein nicht unterliegen, da sich die Verpflichtungen des TKG nur an einen Telekommunikationsdiensteanbieter richten.

[1184] Siehe § 2 Nr. 3 TKÜV und § 1 Abs. 1 Nr. 1 des G-10-Gesetzes, § 100b Abs. 3 Satz 1 der StPO, § 23 b Zollfahndungsdienstegesetz.
[1185] Siehe S. 238 ff.

B. Provider - Nutzer

Die nachfolgenden Ausführungen befassen sich mit den Pflichten im Personenverhältnis zwischen Provider und Nutzer. Es erfolgt zunächst eine Definition des Nutzerbegriffs sowie eine Stellungnahme im Hinblick auf die rechtliche Einordnung der Dienste (siehe unter I.). Die datenschutzrechtliche Prüfung wird sodann (entsprechend der Aufbaulogik dieser Arbeit) im Anschluss vorgenommen (siehe unter II.).

I. Rechtliche Einordnung der Dienste im VPN

Bezüglich des Begriffs des Nutzers wurde darauf hingewiesen, dass dieser unterschiedliche Bedeutungen haben kann.[1186] Im Kontext zum Provider umfasst dieser Begriff denjenigen Personenkreis, dem der VPN-Auftraggeber das VPN oder den Zusatzdienst E-Mail zur Nutzung bereitstellt, insbesondere also dessen Mitarbeitern. Es gilt, dass sämtliche Dienste, die der Provider dem VPN-Auftraggeber zur Verfügung stellt, durch diesen lediglich an seine Mitarbeiter „weitergereicht" werden. Gemäß § 3 Nr. 14 TKG sind die Mitarbeiter damit ebenfalls Nutzer der innerhalb des VPN bereitgestellten Telekommunikationsdienste. Dementsprechend erfahren die jeweiligen bereitgestellten Dienste keine andere rechtliche Bewertung als die, die in dem Personenverhältnis zwischen Provider und VPN-Auftraggeber bereits dargestellt wurde.[1187] Eine gesonderte rechtliche Prüfung der einzelnen Dienste kann daher in dem hier untersuchten Personenverhältnis unterbleiben.

Der Provider erbringt aber durch die Bereitstellung des Internetzugangs sowie des E-Mail-Dienstes ebenso gegenüber dem jeweiligen Kommunikationspartner einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG. Denn als Nutzer des erbrachten Dienstes gemäß § 3 Nr. 24 TKG wird in dieser Arbeit darüber hinaus ebenso derjenige betrachtet, der auf der „gegenüberliegenden Kommunikationsseite" steht. Damit ist zum einen der Inhaber der Ziel-Domain-Adresse bzw. der Website-Betreiber gemeint, der im Verhältnis zum Provider Nutzer des Telekommunikationsdienstes gemäß § 3 Nr. 14 TKG ist. Zum

[1186] Siehe S. 83.
[1187] Siehe S. 121 ff.

anderen ist ebenso der Empfänger einer E-Mail Nutzer des Telekommunikationsdienstes gemäß § 3 Nr. 14 TKG, den der Provider (des VPN-Auftraggebers) durch die Weiterleitung der E-Mail gemäß § 3 Nr. 24 TKG anbietet. Die Bezeichnung „Nutzer“ ist in diesem Kontext gerechtfertigt, da er die seitens des Provider bereitgestellte Internetverbindung ebenfalls in Anspruch nimmt, ohne aber notwendigerweise einen Vertrag mit ihm geschlossen zu haben. Beim E-Mail-Verkehr ist dies mit der Sachlage eines Angerufenen beim Telefonverkehr vergleichbar ist.[1188]

II. Datenschutz innerhalb der Dienste im VPN

Im Personenverhältnis „Provider/VPN-Auftraggeber“ wurden die datenschutzrechtliche Pflichten der Datenvermeidung, technischen Schutzmaßnahmen sowie Auskunft- und Überwachungsmaßnahmen im Rahmen der bereitgestellten Telekommunikationdienste detailliert geprüft.[1189]

Gegenstand der nachfolgenden Betrachtung ist nun, welche eigenständigen datenschutzrechtlichen Pflichten dem Provider im Rahmen der (dem VPN-Auftraggeber) bereitgestellten Dienste (darüber hinaus) gegenüber dem jeweiligen Nutzer obliegen können. Die datenschutzrechtliche Prüfung konzentriert sich daher auf „nutzerspezifische“ Problemstellungen, die wie folgt dargestellt werden:

1. Internetverbindung

Im Rahmen der Bereitstellung der Internetverbindung interessiert vor allem die Frage, welche Anforderungen an einen Einzelverbindungsnachweis gemäß § 99 TKG zu stellen sind.[1190] Diese Thematik wurde bereits im Personenverhältnis „Provider/VPN-Auftraggeber angesprochen.[1191] Hier muss nun die ergänzende Frage gestellt werden, ob und welche

[1188] Vgl. auch die Begründung zum TKG-E S. 120 (zu § 91 TKG).
[1189] Siehe S. 106 ff, 162 ff.
[1190] Siehe zum Einzelverbindungsnachweis Büchner in: TKG-Kommentar, § 6 TDSV (Anh § 89 TKG) Rn. 6, Wittern in: TKG-Kommentar (3. Auflage), § 99 TKG Rn. 1 ff.
[1191] Siehe die Ausführungen auf S. 183 ff., die sich mit der Frage befassen, inwieweit den Provider die Verpflichtungen des § 97 Abs. 4 TKG treffen.

datenschutzrechtlichen Pflichten den Provider unmittelbar gegenüber dem jeweiligen Nutzer treffen. Bei den Nutzern ist zwischen Mitarbeitern und den Kommunikationspartnern (Inhaber eines Ziel-Domain-Namens) wie folgt zu unterscheiden.

a. Mitarbeiter

Ist der Provider im Rahmen der Bereitstellung des Internetzugangs verpflichtet, Datum, Uhrzeit, Dauer der Verbindung sowie Ziel-Domain im Sinne einer Nutzungsübersicht auf Verlangen des Teilnehmers gemäß § 97 Abs. 4 TKG, § 99 TKG aufzulisten, muss er sich unter Berücksichtigung von § 99 Abs. 1 S. 2 TKG seitens des VPN-Auftraggebers eine Erklärung in Textform[1192] vorlegen lassen, dass die entsprechenden Nutzer informiert sind und zukünftige Nutzer informiert werden.[1193]
In rechtspolitischer Hinsicht ist diesbezüglich anzumerken, dass die Regelung des § 99 TKG die Interessen der Nutzer nicht differenziert genug berücksichtigt. Die Erklärung des Teilnehmers gegenüber dem Anbieter des Telekommunikationsdienstes, mögliche „Mitbenutzer“ über die Verwendung eines Einzelverbindungsnachweises (nur) zu informieren, ist nicht in allen Fällen nicht interessengerecht. Hier hätte zwischen dienstlicher und privater Nutzung unterschieden werden müssen, was aber erst im Personenverhältnis „VPN-Auftraggeber/Nutzer“ deutlich wird. Auch aus diesem Grunde ist wiederum die Gesamtbetrachtung der Personenverhältnisse erforderlich.[1194]

Ergänzend soll hier außerdem folgendes angemerkt werden: Sofern Domain-Namen (entgegen der hier vertretenen Auffassung) nicht als Nummern gemäß § 3 Nr. 13 TKG eingeordnet werden,[1195] so würde dies dazu führen, dass § 99 TKG für die Frage der Zulässigkeit dieses Sachverhalts keine Anwendung finden würde. Eine „reine“ Informationspflicht wäre daher nicht ausreichend. Insgesamt müsste also in diesem Falle zum Schutze der Nutzer eine

[1192] Zur Textform siehe § 126 b BGB. Danach reicht grundsätzlich auch eine E-Mail aus (vgl. Kath/Riechert, Internet-Vertragsrecht, Rn. 220).
[1193] Siehe zu den Tatbestandsvoraussetzungen des § 99 TKG Wittern in: TKG-Kommentar (3. Auflage), § 99 TKG Rn. 8 ff.
[1194] Siehe S. 327 ff. sowie S. 333 ff.
[1195] Siehe Holznagel, MMR 2003, 219, 221. Siehe außerdem die Ausführungen auf S. 183 ff./188 ff.

entsprechende Erklärung des VPN-Aufragebers in Textform dahingehend gefordert werden, dass die Nutzer in die vollständige Speicherung der Domain-Namen gemäß § 4a BDSG eingewilligt haben.

b. Inhaber der Ziel-Domain-Adresse

Der Inhaber der Ziel-Domain-Adresse bzw. der Website-Betreiber ist im Verhältnis zum Provider Nutzer des Telekommunikationsdienstes gemäß § 3 Nr. 14 TKG, da er die seitens des Provider bereitgestellte Internetverbindung ebenfalls in Anspruch nimmt, ohne aber notwendigerweise einen Vertrag mit diesem Provider geschlossen zu haben. Speichert der Provider gemäß § 97 Abs. 4 TKG die „angewählten" Ziel-Domain oder IP-Adresse sowie nähren Verbindungsdaten stellt sich die Frage, inwieweit den Provider ebenso datenschutzrechtliche Verpflichtungen gegenüber dem Inhaber dieser Ziel-Domain treffen. Diese Frage soll der vollständigkeithalber geprüft werden, auch wenn sie in der Praxis keine besondere Relevanz hat. Für einen Provider ist es bereits aus Gründen der Speicherkapazität regelmäßig nicht möglich, die Ziel-IP-Adressen zu speichern.
Ob dem Provider gegenüber dem Inhaber der Ziel-IP-Adresse besondere Unterrichtungspflichten gemäß § 93 TKG in Betracht obliegen,[1196] ist außerdem nur im Rahmen des freiwilligen Tunneling von Bedeutung. Ansonsten (beim zwangsweisen Tunneling) kann ein Verbindungsaufbau ohnehin lediglich zwischen den Standorten stattfinden.[1197]
Die Gesetzesbegründung zur TDSV und dem TKG legt den Schluss nahe, dass mit der Informationspflicht des § 93 S. 3 TKG gegenüber Nutzern an Fälle gedacht wurde, in denen nicht nur die Daten der unmittelbaren Vertragspartner (Teilnehmer), sondern ggf. auch Rufnummern angerufener Teilnehmer gespeichert werden.[1198] Dies betrifft also Sachverhalte, in welchen eine unmittelbare Unterrichtung bei Vertragsabschluss nicht möglich ist. Ausreichend sollen daher insoweit allgemeine Informationen sein, etwa durch Hinweise in Teilnehmerverzeichnissen.

[1196] Siehe zu den allgemeinen Unterrichtungspflichten S. 110 ff.
[1197] Siehe S. 57 ff.
[1198] Vgl. hierzu Begründung zum TKG-E, S. 43.

Hieran zeigt sich, dass das TKG (sowie zuvor die TDSV) vorrangig für Telefonverbindungen konzipiert wurden. Teilnehmerverzeichnisse gibt es für Online-Vorgänge bislang nicht. Daher muss eine entsprechende Unterrichtung bezüglich der erhobenen und gespeicherten Daten durch jeden einzelnen Provider (beispielsweise in den jeweiligen Datenschutzhinweisen) erfolgen. Problematisch ist dabei, dass dem Nutzer nicht bekannt ist, über welchen Provider die Online-Verbindung zu seinem Server aufgebaut wird. Daher ist ihm letztendlich nicht bekannt, welche Daten der jeweilige Provider speichert. Eine Unterrichtung der Nutzer gemäß § 93 S. 3 TKG kann daher bei einem VPN lediglich im Rahmen des zwangsweisen Tunneling in Betracht kommen, da in diesem Falle dem Provider sämtliche Nutzer bekannt sind.[1199]
Beim freiwilligen Tunneling hingegen (wenn der Verbindungsaufbau nicht an Standorte des VPN gebunden ist) ist eine Unterrichtung der Nutzer aus den gerade genannten Gründen nahezu unmöglich. Zu beachten ist jedoch, dass der Inhaber der Ziel-Domain bei einer Speicherung datenschutzrechtlich ohnehin nicht betroffen wäre.
So ist die Einseitigkeit des Verbindungsaufbaus zu berücksichtigen. Es erfolgt anders als beim E-Mail-Verkehr oder bei einem Telefonat regelmäßig keine persönliche bidirektionale Kommunikation. Damit sind Rechte des Website-Inhabers nicht betroffen, sofern dokumentiert wird, wann, von wem und für welche Dauer seine Website aufgerufen worden ist.[1200] Mangels eigener Aktivität wird in das Fernmeldegeheimnis des Server-Betreibers gemäß § 88 TKG regelmäßig nicht eingegriffen. Allein durch die offene Anbindung seines Servers ans Internet ist er unterschiedlichen Zugriffen „ausgesetzt“, die keine Aussagekraft bezüglich seines eigenen Kommunikationsverhaltens haben. Umgekehrt könnte man auch sagen, dass sich der Inhaber eines Ziel-Domain-Namens durch ständige Anbindung an das Internet bewusst dafür entschieden hat, stets an einem Kommunikationsvorgang beteiligt zu sein. Dies stellt im Sinne von § 88 TKG bei Internetauftritten aber kein Geheimnis dar. Im Gegensatz zu E-Mail-Adressen, die nicht stets ohne weiteres auffindbar sind, sind Domains durch jede Suchmaschine leicht zu finden.[1201] Lediglich bei einem VPN kann die Tatsache, dass überhaupt eine Internetanbindung des Standorts

[1199] Siehe S. 57 ff.
[1200] Vgl. zur datenschutzrechtlichen Relevanz (aus der Sicht des Angerufenen) bei Speicherung seiner Telefonnummer Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 98.
[1201] Siehe Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 98 zum Datenschutz des Angerufenen.

für einen kleineren Benutzerkreis erfolgt, das Fernmeldegeheimnis gemäß § 88 TKG berühren. In diesem Falle ist dem Betreiber eines VPN bzw. dem VPN-Auftraggeber jedoch bereits bekannt, ob Ziel-Domains oder Ziel-IP-Adressen gespeichert werden, so dass wegen dieser Kenntnis eine Unterrichtung unterbleiben kann.

Hiervon unabhängig ist die Frage zu beurteilen, ob der Arbeitnehmer oder VPN-Auftraggeber durch die Speicherung des Ziel-Domain-Namens in seinen Rechten verletzt ist. Denn in diesem Falle wäre das Surfverhalten nachvollziehbar.[1202]

2. Zwangsweises Tunneling

Ein weiteres datenschutzrechtliches Problem ergibt sich in dem hier untersuchten Personenverhältnis „Provider und Nutzer" im Rahmen des zwangsweisen Tunneling.[1203] Es stellt sich zwischen Provider und einem Nutzer, der Mitarbeiter des VPN-Auftraggebers ist, die Frage, ob beim zwangsweisen Tunneling „nur" eine Auftragsdatenverarbeitung gemäß § 11 BDSG in Betracht kommen kann, oder ob hier nicht vielmehr eine Funktionsübertragung[1204] anzunehmen ist. Dieser Punkt muss im Übrigen nicht bezüglich eines externen Nutzers (beispielsweise eines Lieferanten) geprüft werden, da ein Externer regelmäßig einen eigenständigen Vertrag mit einem Access-Provider abgeschlossen hat.
Im Hinblick auf Mitarbeiter ist die Frage jedoch aus dem Grunde relevant, da der Provider an seinem Internetzugangsknoten, wie beispielsweise dem PoP, und der dazu gehörigen Datenbank Nutzerdaten verarbeitet und die Voraussetzungen für das zwangsweise Tunneling schafft.[1205] Im Falle einer Funktionsübertragung ist die Datenverarbeitung, unabhängig davon, ob die Bearbeitung durch eine öffentliche oder private Stelle und ob sie im Weg der Delegation oder des Mandat wahrgenommen werden soll, nur auf der

[1202] Vgl. hierzu S. 183 ff./281 ff.
[1203] Vgl. die Ausführungen auf S. 57 ff.
[1204] Vgl. Gola/Schomerus, BDSG, § 11 BDSG Rn. 9. Siehe auch Wächter, CR 1991, 333, 333, der eine Funktionsübertragung dann bejaht, wenn neben der Datenverarbeitung auch die zugrundeliegende Aufgabe übertragen wird. Siehe zur Funktionsübertragung insbesondere die Ausführungen auf S. 382 ff
[1205] Vgl. die Ausführungen auf S. 57 ff.

Grundlage einer gesetzlichen Regelung, etwa § 28 BDSG, zulässig.[1206] Daher wird im Folgenden untersucht, ob die Leistung des zwangsweisen Tunneling als Auftragsdatenverarbeitung gemäß § 11 BDSG oder als Funktionsübertragung zu qualifizieren ist.

Sofern der Auftrag zum zwangsweisen Tunneling durch den VPN-Auftraggeber an den Provider nicht konkret ausgestaltet ist, sondern allein dahingehend erfolgt, dass zwangsweises Tunneling sicherzustellen ist (egal wie), dann entscheidet der Provider selbständig auf welche Art und Weise er die entsprechenden Voraussetzungen schafft. So hängt es von der Konkretisierung des Auftrags ab, ob eine Auftragsdatenverarbeitung vorliegt.[1207]
Eine Auftragsdatenverarbeitung liegt dann vor, sofern der Dienstleister unselbständig tätig ist und den Weisungen des Auftraggebers unterworfen ist, quasi als sein verlängerter Arm fungiert, und sich der Auftragsschwerpunkt in erster Linie auf die technische Durchführung der Datenverarbeitung richtet.[1208]

Eine Funktionsübertragung kommt hingegen in Betracht, wenn die Aufgabe des Dienstleisters nicht nur darin besteht, für die Einsatzbereitschaft seines Systems Sorge zu tragen, sondern über die weisungsabhängige technische Datenverarbeitung hinausgeht.[1209] Dies liegt vor, wenn dem Provider bzw. Dienstleister nicht allein die Verarbeitung der Daten übertragen wird, sondern vielmehr eine gesamte Aufgabe, zu deren Erfüllung die Verarbeitung der Daten notwendig ist,[1210] so dass ihm eigene Entscheidungsbefugnisse hinsichtlich des

---

[1206] Siehe Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 92; Gola/Schomerus, BDSG, § 28 BDSG Rn. 5. Im Übrigen kommt die Anwendbarkeit des TKG bei der Frage der Zulässigkeit der Speicherung der Benutzerkennungen nicht in Betracht, vgl. S. 226 ff.
[1207] Gola/Schomerus, BDSG, § 11 BDSG Rn. 9. Wronka, RDV 2003, 132, 135 stellt klar, dass die Fragestellung der Auftragsdatenverarbeitung oder Funktionsübertragung von den durch vertragliche Absprachen zum Ausdruck gebrachten Interessenlage des Auftraggebers abhängt. Vgl. außerdem Kramer/Herrmann, CR 2003, 938, 938; Evers/Keine, NJW 2003, 2726, 2727; Steding, BB 2001, 1693, 1698.
[1208] Wronka, RDV 2003, 132, 132. Vgl. auch Kramer/Herrmann, CR 2003, 938, 938 sowie Dolderer/v.Garrel/Müthlein/Schlumberger, RDV 2001, 223, 224 zur Funktion des Auftragnehmers als „verlängerter Arm".
[1209] Vgl. hierzu auch Müthlein/Heck, Outsourcing und Datenschutz, S. 34 ff. mit dem Hinweis auf S. 35, dass eine Einzelfallbetrachtung für die Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung notwendig ist; Niedermeier/Schröcker, RDV 2001, 90, 92. Steding, BB 2001, 1693, 1699 ff. Siehe zu den Voraussetzungen einer Funktionsübertragung in Abgrenzung zur Auftragsdatenverarbeitung auch Räther, DuD 2005, 461, 465.
[1210] Vgl. Geis, Recht im eCommerce, S. 74, der eine Funktionsübertragung dann annimmt, wenn die Aufgabe zur selbständigen Erledigung übertragen wird und der Datenverarbeiter

„Wie“ und der Auswahl der Daten zustehen, und er selbständig ohne Weisungen des Auftraggebers arbeitet.[1211]

Im Sinne dieser Definitionen ist beim zwangsweisen Tunneling regelmäßig von einer Funktionsübertragung auszugehen, wenn der Provider seitens des VPN-Auftraggebers den Auftrag erhält, zwangsweises Tunneling sicherzustellen, und eigenständig darüber entscheiden kann, ob er dem VPN-Auftraggeber und dessen Nutzern Einwahlnummern, ziffernmäßige Kennungen oder die Preisgabe von Namen und gegebenenfalls dienstlichen Funktionen der Nutzer verlangt. In der Regel wird ein Provider einem VPN-Auftraggeber eigene technische Systeme und Lösungen präsentieren, ohne dass der VPN-Auftraggeber noch wesentliche Änderungen verlangen könnte, so dass die Entscheidung über die konkrete Gestaltung und Durchführung bereits festgelegt ist.

Zu berücksichtigen ist ebenso, dass der VPN-Auftraggeber nicht das technische Know-How hat, um im Einzelfall für die Datenverarbeitung konkrete Weisungen zu erteilen.
In diesem Falle besteht die Aufgabe des Providers nicht nur darin, für die Einsatzbereitschaft seines Systems Sorge zu tragen, sondern geht darüber hinaus.[1212] Dem Provider wird damit nicht allein die Verarbeitung der Daten übertragen, sondern vielmehr die gesamte Aufgabe „zwangsweises Tunneling“, zu deren Erfüllung die Verarbeitung der Daten notwendig ist.[1213] Der Provider hat eigene Entscheidungsbefugnisse hinsichtlich des „Wie“ und der Auswahl der Daten inne, und er arbeitet selbständig ohne Weisungen des Auftraggebers,

---

selbst bestimmen kann, welche Arten personenbezogener Daten gespeichert oder verarbeitet werden. In diesem Sinne ebenso Niedermeier/Schröcker, RDV 2001, 90, 93 und Schneider, Handbuch des EDV-Rechts, Teil B Rn. 448.

[1211] Vgl. Kramer/Herrmann, CR 2003, 938, 939. Wächter, CR 1991, 333, 334 verweist für die Auftragsdatenverarbeitung auf die notwendigen Weisungen des Auftraggebers als „verbindliche Richtschnur“ des Handelns des Auftragnehmers. Siehe auch Niedermeier/Schröcker, RDV 2001, 89, 92; v.Westphalen, WM 1999, 1810, 1815.

[1212] Vgl. hierzu auch Müthlein/Heck, Outsourcing und Datenschutz, S. 34 ff.

[1213] Vgl. auch Geis, Recht im eCommerce, S. 74, der eine Funktionsübertragung dann annimmt, wenn die Aufgabe zur selbständigen Erledigung übertragen wird und der Datenverarbeiter selbst bestimmen kann, welche Arten personenbezogener Daten gespeichert oder verarbeitet werden.

so dass seine Dienstleistung über die weisungsabhängige technische Datenverarbeitung hinausgeht.[1214]
Damit ist der VPN-Auftraggeber nicht mehr „Herr der Daten".[1215] Somit gilt, dass für die Übermittlung (§ 3 Abs. 4 Nr. 3 BDSG) der personenbezogenen Daten der Nutzer an den Provider besondere Voraussetzungen bezüglich der Zulässigkeit gelten. Der Nutzer muss entweder gemäß § 4a BDSG in die Übermittlung seiner Daten einwilligen, oder die Zulässigkeit muss sich aus § 28 BDSG ergeben.
§ 28 Abs. 1 Nr. 1 BDSG kommt allerdings nicht in Betracht, da die Übermittlung nicht der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichem Vertrauensverhältnisses mit dem Nutzer dient. Dienen ist hierbei im Sinne eines „Müssen" zu verstehen.[1216] Die Einführung des zwangsweisen Tunneling ist für das Arbeitsverhältnis zwischen VPN-Auftraggeber und Nutzer jedoch nicht im Sinne eines „Muss" erforderlich.
Eine weitere Alternative ist die zulässige Übermittlung durch die Anwendung von § 28 Abs. 1 Nr. 2 BDSG zu legitimieren. So stellt das zwangsweise Tunneling ein berechtigtes Interesse des VPN-Auftraggebers dar, da unter einem berechtigten Interesse gemäß § 28 Abs. 1 Nr. 2 BDSG jedes Interesse wirtschaftlicher oder ideeller Natur fallen kann.[1217]
Fraglich ist allerdings, ob nicht die berechtigten Interessen des Nutzers dieser Datenübermittlung entgegenstehen könnten. Für diese Bewertung ist zu berücksichtigen, dass es beim zwangsweisen Tunneling unterschiedliche technische Methoden, um die Standortverbindung sicherzustellen. Eine Methode beinhaltet, dass an die Namen der einzelnen Nutzer Präfixe oder Suffixe angehängt werden.[1218] Dies stellt eine technische Variante dar, auf welche regelmäßig verzichtet werden sollte, sofern es Möglichkeiten gibt, das zwangsweise Tunneling auf andere Art und Weise sicherzustellen. Denn auch hier stellt sich die vorrangige Frage, ob personenbezogene Daten überhaupt verarbeitet werden müssen.[1219]

[1214] Niedermeier/Schröcker, RDV 2001, 90, 92.
[1215] Vgl. oben Fn. 1002 und Gola/Schomerus, BDSG, § 11 BDSG Rn. 3.
[1216] Siehe Gola/Schomerus, BDSG, § 28 BDSG Rn. 13, mit dem Hinweis, dass ein „verarbeiten müssen" zu fordern ist, auch wenn der Gesetzeswortlaut lediglich ein „dienen" erfasst.
[1217] Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 85; Simitis in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 139.
[1218] Siehe S. 59 ff.
[1219] Siehe zur Datenvermeidung auch S. 106

Für den VPN-Auftraggeber stellen die Namen der Nutzer, an welche Präfix oder Suffix angehängt sind, personenbezogene Daten dar, selbst wenn sie abgekürzt werden, wie etwa aschmidt@unternehmen-x.de oder smueller-vertrieb@unternehmen-x.de. Dies kommt für den Provider zwar nicht unter allen Umständen in Betracht, da regelmäßig faktische Anonymität vorliegt.[1220] Dem Provider ist in dem gerade genannten Beispiel unter Umständen nur bekannt, dass ein ASchmidt bei Unternehmen X arbeitet, ohne aber nähere Details, etwa Adressdaten, über ihn zu wissen. Wie bereits ausgeführt liegt eine vollständige Anonymität nur dann vor, wenn der Personenbezug tatsächlich im Sinne von § 3 Abs. 6 1. Alt BDSG beseitigt wird.[1221] Eine Anonymität kann aber nach der in dieser Arbeit vertretenen Auffassung nicht vorliegen, sofern zwei verarbeitende Stelle lediglich ihr Wissen austauschen müssten.[1222] Es bestehen zudem vielfältige Möglichkeiten der Zusammenführung von Daten im Internet,[1223] wobei es nicht angemessen ist, Anonymität auch dann zu bejahen, sofern die Bestimmbarkeit einer Person tatsächlich vorliegt, die entsprechende Kenntnis aber mit illegalen Mitteln erworben worden ist.[1224]
Daher ist im Einklang mit dem Systemdatenschutz gemäß § 3a BDSG zu fordern, dass dort, wo es technisch machbar ist, auf die Speicherung von Benutzernamen in der Datenbank des Providers verzichtet wird, da in diesem Fall dem Umstand Rechnung getragen werden kann, so wenig wie möglich personenbezogene Daten zu verwenden. So ist etwa die Vergabe einer Einwahlnummer[1225] oder aber verschiedener Benutzerkennungen ohne einen Namensbezug möglich. Der Provider benötigt keine näheren Angaben über die einzelnen Nutzer eines VPN. Ausreichend wäre, dem Kunden für die

[1220] Siehe zur faktischen Anonymität S. 106 ff.
[1221] Siehe S. 106 ff. sowie S. 215 ff..
[1222] Siehe die Verweise in den vorstehenden Fußnoten.
[1223] Siehe hierzu im Besonderen auch Schaar, Datenschutz im Internet, Rn. 174, der im Hinblick auf die IP-Adresse ausführt, dass mit Hilfe von Dritten, die für die Zuweisungen der Adressen zuständig sind, bereits jetzt ohne unverhältnismäßigen Aufwand möglich ist, einen Internetnutzer aufgrund seiner IP-Adresse zu identifizieren. Eine Betrachtungsweise, die ausschließlich auf die Möglichkeiten einer verantwortlichen Stelle (z.B. Content Provider) abstelle, die Identifizierung selbst vorzunehmen, sei verkürzt und trage der vielfältigen Möglichkeiten zur Zusammenführung personenbezogener Daten im Internet nicht Rechnung. Dies würde dem Schutzgedanken des Datenschutzrechts diametral entgegenlaufen. Insbesondere sei auch zur berücksichtigen (Rn. 175), dass die Möglichkeit zur nachträglichen Ermittlung der Nutzer durch Zuordnung von IP-Nummern von Strafverfolgungsbehörden verstärkt in Anspruch genommen werde, so dass im Grunde kein Zweifel daran bestehen dürfe, dass Daten über Internetnutzung, die zusammen mit der IP-Nummer gespeichert wurden, personenbezogen sind.
[1224] Siehe oben S. 215 ff.
[1225] Siehe oben S. 57 ff.

Netzeinwahl unterschiedliche Ziffernkombinationen zur Verfügung zu stellen, so dass die Preisgabe von Benutzernamen letztendlich nicht erforderlich ist. Das Unternehmen könnte diese Ziffernkombinationen selbständig an seine Nutzer weitergeben, so dass für einen Provider letztendlich für seine Diensterbringung allein die anonyme Anzahl der Mitbenutzer entscheidend ist.
Auch wenn im Rahmen des zwangsweisen Tunneling sämtliche Nutzer eine gleiche Einwahlnummer erhalten, durch die sie automatisch zu dem gewünschten Standort geleitet werden, dann sind und bleiben die Nutzer für den Provider und ebenso für Dritte, die in unberechtigerweise auf das System Zugriff nehmen, auf jeden Fall „anonymer".

Nachteilig ist für den VPN-Auftraggeber insoweit, dass sich die Zulässigkeit der Datenverarbeitung, d.h. der Verknüpfung der Daten, nicht nach dem TKG, sondern nach dem BDSG richtet.[1226] Dies bedeutet, dass dem Provider gemäß § 93 S. 2 TKG keine Unterrichtungspflichten über die unterschiedlichen Wahl- und Gestaltungsmöglichkeiten obliegen, so dass der VPN-Auftraggeber sich selbständig entscheiden und kundig machen muss, welche unterschiedlichen technischen Möglichkeiten in Frage kommen.[1227]

Die obigen Ausführungen zeigen jedoch, dass die Übermittlung von personenbezogenen Nutzerdaten zum Zwecke der Bereitstellung des zwangsweisen Tunneling durch einen Provider Einschränkungen unterliegt. Die Übermittlung ist nur in den Fällen zulässig, in denen sorgfältig abgewogen wurde, dass die schutzwürdigen Interessen der Nutzer nicht entgegenstehen. Gibt es –wie oben dargestellt- andere Alternativen als die Übermittlung von personenbezogenen Daten der Nutzer, so kommt der Tatbestand des § 28 Abs. 1 Nr. 2 BDSG nicht in Betracht, da die schutzwürdigen Interessen gegen eine Weitergabe der Daten sprechen. In diesen Fällen muss vielmehr die ausdrückliche Einwilligung des Nutzers gemäß § 4a BDSG eingeholt werden.

[1226] Vgl. auch S. 226 ff.
[1227] Siehe auch Büchner in: TKG-Kommentar (2. Auflage), § 3 TDSV (Anh § 89 TKG) Rn. 4 mit dem Hinweis, dass die Unterrichtungspflicht im Rahmen von Telekommunikationsdiensten über die Benachrichtigungspflicht des § 33 BDSG hinausgeht, da diese sich lediglich auf die Speicherung bezieht. Die Unterrichtungspflichten des § 3 Abs. 4 TDSV a.F., die nunmehr in § 93 TKG geregelt sind, umfassen darüber hinaus transparente Hinweise über das Wie einer Verarbeitung und Nutzung entsprechender Daten (Büchner aaO). Siehe auch Büttgen in: TKG-Kommentar (3. Auflage), § 93 TKG Rn. 24 mit dem Hinweis, dass mit der Einführung von § 93 TKG keine inhaltliche Änderung zu der Regelung des § 3 Abs. 5 TDSV verbunden ist.

Dies ist sowohl vom Provider als auch vom VPN-Auftraggeber zu beachten.

Hier zeigt sich wiederum, dass die Betrachtung des Mehrpersonenverhältnisses sowie die Betrachtung der Datenverarbeitung auf dem konkreten System für eine datenschutzrechtliche Prüfung notwendig sind.

3. VPN-Kommunikation und Gatewaymanagement

a. Datenvermeidung

Sofern der Provider das Management des Gateways übernimmt,[1228] liegt gleichfalls eine Funktionsübertragung an den Provider vor, wenn er in eigenständiger Weise über die Verwendung der Daten im Rahmen der Benutzerauthentifizierung entscheiden kann. Die an dem Gateway vorzunehmende[1229] Benutzerauthentifizierung muss der Provider demgemäß im Sinne eines ausreichenden Systemdatenschutzes gemäß § 3a BDSG gewährleisten. Dies gilt unabhängig davon, ob sich der Gateway im Einflussbereich des VPN-Auftraggebers oder des Providers befindet, sofern der Provider hier selbständig entscheiden kann, auf welche Art und Weise er die Benutzerauthentifizierung hier vornimmt. Sofern sich der Gateway im Einflussbereich des VPN-Auftraggebers befindet, aber die Benutzerverwaltung dem Provider übertragen ist, übt zwar der VPN-Auftraggeber die Funktionsherrschaft über diesen Gateway aus, stellt eigene Telekommunikation gemäß § 3 Nr. 22 TKG bereitstellt und erbringt einen eigenständigen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG.[1230] Nichtsdestotrotz kann sich im Hinblick auf die Datenverarbeitung auf dem Gateway hiervon abweichend ergeben, dass der Provider diese weisungsunabhängig und ohne konkrete Vorgaben des VPN-Auftraggebers vornimmt. Auch hier kann im Einzelfall die Annahme gerechtfertigt sein, dass der VPN-Auftraggeber dem Provider aufgrund seines technischen Wissensvorsprungs „blind“ vertraut und ihm die Entscheidung über das Wie und die Auswahl der Daten bei der Benutzerauthentifizierung überlässt.

[1228] Siehe S. 49 (Systemmanagement durch den Provider).
[1229] Vgl. S. 46 ff.
[1230] Vgl. hierzu S. 149 ff.

Der Provider kann dementsprechend bezüglich der Datenverarbeitung, die sich nach dem BDSG richtet, eigenständige Funktionen wahrnehmen, so dass die Funktionsherrschaft über eine Telekommunikationsanlage nicht zwangsläufig Herrschaft über die verarbeiteten Daten bedeutet. Es muss vielmehr unter Berücksichtigung des konkreten Einzelfalles stets eigenständig untersucht werden, inwieweit eine Auftragsdatenverarbeitung gemäß § 11 BDSG oder eine Funktionsübertragung vorliegt.
Dies hat Auswirkungen auf die Pflichten im Hinblick auf den Betroffenen, die in den weiteren Personenverhältnissen zwischen „VPN-Auftraggeber/Betroffener" sowie „Provider/Betroffener" zu prüfen sind. [1231]

b. Technische Schutzmaßnahmen

Gegenüber dem VPN-Auftraggeber treffen den Provider die Verpflichtungen gemäß §§ 109 Abs. 1, 109 Abs. 2 TKG,[1232] sofern er gemäß § 3 Nr. 6 TKG Anbieter eines Telekommunikationsdienstes ist und/oder die Funktionsherrschaft über den Gateway innehat.[1233] Im Hinblick auf den Nutzer obliegen ihm diese Pflichten nur, sofern dieser ebenso in seinem Fernmeldegeheimnis gemäß § 88 TKG oder in seinen personenbezogenen Daten gemäß § 109 Abs. 1 Nr. 1 TKG betroffen ist.[1234]
Denn zu beachten ist, dass die Pflichten des § 109 TKG nicht nur den Schutz des Teilnehmers bezwecken, sondern der Wortlaut des § 109 TKG vielmehr allgemein gehalten ist. Insbesondere nimmt § 109 Abs. 1 Nr. 1 TKG auf das Fernmeldegeheimnis gemäß § 88 TKG Bezug, welches nutzer- bzw. drittschützenden Charakter hat.[1235]

[1231] Vgl. hierzu S. 436 ff./449 ff.
[1232] Siehe S. 250 ff.
[1233] Siehe S. 49 (Systemmanagement durch den Provider) und S. 51 (Splitmanagement – Einflussbereich des Providers).
[1234] Vgl. auch Büchner in: TKG-Kommentar (2. Auflage), § 40 TKG Rn. 5 zum nutzer-bzw. drittschützenden Charakter des § 87 Abs.1 TKG a.F. (technische Schutzmaßnahmen); siehe zu den Schutzzielen des § 109 TKG (§ 87 TKG a.F) Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 25/26. Ebenso Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 40 TKG(1998), Band 1, Rn. 8.
[1235] Siehe zum drittschützenden Charakter des Fernmeldegeheimnisses Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 23; K. Lau in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 88 TKG(2004), Band 2, Rn. 90; siehe zum persönlichen Schutzbereich des Fernmeldegeheimnisses Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 19; siehe ebenso Zerres in: Scheurle/Mayen, TKG-Kommentar, § 85 TKG Rn. 20, der den Schutz des Fernmeldegeheimnisses auf sämtliche Telekommunikationsteilnehmer erstreckt. Ebenso Haß in: Manssen, Kommentar

Allerdings ist hier die Überlegung mit einzubeziehen, dass regelmäßig nur ein Nutzer in seinem Fernmeldegeheimnis gemäß § 88 TKG betroffen ist, dessen Kommunikation nicht dem VPN-Auftraggeber zuzurechnen ist, sondern vielmehr eigenständig zu bewerten ist. Unterlässt der Provider beispielsweise notwendige Sicherheitsmaßnahmen, so dass für einen außenstehenden Dritten nachvollziehbar wird, dass und mit welchem Inhalt ein bestimmter Mitarbeiter innerhalb des VPN kommuniziert hat, so liegt regelmäßig keine Verletzung des Fernmeldegeheimnisses des Mitarbeiters vor. Ein VPN soll gerade den Zweck der sicheren geschäftlichen Kommunikation erfüllen. Damit ist die Kommunikation dem Arbeitgeber zuzurechnen, so dass dieser in seinem Fernmeldegeheimnis verletzt ist. Etwas anderes gilt nur, wenn der Nutzer private Inhalte austauschen sollte.

c. Auskunfts- und Überwachungsmaßnahmen

Auch im Hinblick auf den Nutzer muss der Provider beim Komplettmanagement, welches ebenso die Benutzerverwaltung umfasst,[1236] beachten, dass er eine Kopie der Telekommunikation und eine Aufhebung der Verschlüsselung oder Benutzerauthentifizierung nur vornehmen muss und darf, sofern die Voraussetzungen der TKÜV[1237] oder gemäß § 113 Abs. 1 S. 3 TKG und eine damit verbundene Anordnung nach § 100a StPO, § 100b Abs. 3 StPO, des § 2 Abs. 1 Satz 3 des G-10-Gesetzes, § 23a Abs. 1 S. 1 des Zollfahndungsdienstegesetzes oder nach Landesrecht vorliegen.[1238]
Das Fernmeldegeheimnis hat gemäß § 88 TKG, wie oben festgestellt, nutzer- bzw. drittschützenden Charakter, so dass eine entsprechende Befugnisnorm vorliegen muss.

Telekommunikations- und Multimediarecht, § 85 TKG(1998), Band 1, Rn. 27. In diesem Sinne ebenso Klesczewski in: Berliner Kommentar zum TKG, § 88 TKG Rn. 10, der den personalen Anwendungsbereich zugunsten des „Anrufers“ und des „Angerufenen“ festlegt.

[1236] Siehe S. 49 (Systemmanagement durch den Provider).

[1237] Vgl. hierzu S. 263.

[1238] Siehe hierzu auch die Ausführungen in der Einführung S. 13 und den Hinweis auf Ehmer in: TKG-Kommentar, Anh § 88 TKG, der unter Anmerkung 1 (keine Randnummern vorhanden) ausführt, dass aus den Vorschriften des G-10-Gesetzes folgt, der StPO und des AWG (nunmehr Zollfahndungsdienstegesetz) folgt, dass der Gesetzgeber von der grundsätzlichen Verpflichtung, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, keine Ausnahmen vorgesehen hat. Vgl. auch Kloepfer in: Holznagel/Nelles/Sokol, TKÜV, S. 94/95 mit der Fragestellung, ob der Protest gegen die TKÜV nicht bereits früher hätte ansetzen müssen, und zwar an den Ermächtigungsvorschriften, also §§ 100a, 100b StPO, dem Artikel 1 § 2 des G-10-Gesetzes sowie den §§ 39 ff. AWG (nunmehr Zollfahndungsdienstegesetz).

Für ein VPN bedeutet dies entsprechend der Ausführungen in dem vorangegangenen Prüfungspunkt, dass ein Mitarbeiter regelmäßig nicht in seinem Fernmeldegeheimnis gemäß § 88 TKG und seinen personenbezogenen Daten betroffen ist, sofern die Datenverschlüsselung aufgehoben wird, da die Einrichtung eines VPN und einer Standortverbindung dazu dient, die geschäftliche Kommunikation gesichert zu ermöglichen und dementsprechend seitens des VPN-Auftraggebers entsprechende arbeitsbezogene Dateiordner zum Zugriff freigegeben werden.

Sofern mit einer Anordnung gemäß § 113 Abs. 1 S. 2 TKG i.V.m. §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO auch verbunden ist, dass der Nutzer durch die Aufhebung der Verschlüsselung oder durch die Auskunft über die Benutzerauthentifizierungen[1239] erkennbar einem Unternehmen zugeordnet oder gar seine dortige berufliche Position bestimmt werden kann, gilt, dass der Mitarbeiter nicht in seinem Fernmeldgeheimnis gemäß § 88 TKG, sondern allein in seinen personenbezogenen Daten gemäß § 3 Abs. 1 BDSG betroffen ist.[1240]

In seinem Fernmeldegeheimnis ist lediglich der Nutzer betroffen, der „eigene“ (inhaltliche) Kommunikation führt und nachvollziehbar wäre, zu welchem Zeitpunkt der Nutzer mit wem und für welchen Zeitraum kommuniziert hat.

[1239] Siehe oben S. 261.

[1240] Vgl. zu Einzelangaben des § 3 Abs. 1 BDSG Gola/Schomerus, BDSG, § 3 BDSG Rn. 3; Schulz in: Roßnagel, Recht der Multimedia-Dienste, § 1 TDDSG Rn. 28; Tinnefeld/Ehmann/Gerling Einführung in das Datenschutzrecht, S. 279, insbesondere auch die Ausführungen auf S. 92 ff. in dieser Arbeit nebst Verweisen. Siehe zur Gefährdung der Privatsphäre im Rahmen der Telekommunikationsüberwachung auch Kloepfer in: Holznagel/Nelles/Sokol, TKÜV, S. 108 ff.

4. Zusatzdienst E-Mail

Beim Zusatzdienst E-Mail werden im Personenverhältnis „Provider/Nutzer" die nachfolgenden datenschutzrechtlichen Fragestellungen behandelt. Hierbei ist danach zu unterscheiden, ob es sich bei dem Nutzer um einen E-Mail-Kommunikationspartner des VPN-Auftraggebers oder um einen Mitarbeiter handelt, der seitens des VPN-Auftraggebers den E-Mail-Account bereitgestellt erhält.

a. Datenvermeidung

aa. E-Mail-Kommunikationspartner

Auch der Empfänger einer E-Mail ist gemäß der Auslegung in dieser Arbeit Nutzer des E-Mail-Dienstes.[1241] Bei der Zieladresse des Empfängers handelt es sich im Hinblick auf den konkreten Versendungsvorgang und aus Sicht des Providers, der die Versendung vornimmt, um ein Verkehrsdatum gemäß § 3 Nr. 30 TKG und nicht um ein Bestandsdatum nach § 3 Nr. 3 TKG.[1242] Dies ändert nichts daran, dass die E-Mail-Adresse des Empfängers in einem anderem Zusammenhang oder in einem zwischen Provider und E-Mail-Kommunikationspartner (außerdem bestehenden) Vertragsverhältnis ein Bestandsdatum gemäß § 3 Nr. 3 TKG oder gemäß § 5 TDDSG oder personenbezogenes Datum gemäß § 3 Abs. 1 BDSG darstellen könnte.

Im Hinblick auf den Nutzer, der Empfänger der E-Mail ist, ist der Provider ebenso verpflichtet, die aus Umschlag, Header und Inhalt bestehende E-Mail[1243] bzw. die in einer Logdatei gegebenenfalls entstandene E-Mail-Adresse des Empfängers gemäß § 96 Abs. 2 TKG auf den Systemen, die für den Versand der E-Mail zuständig sind, zu löschen, sofern sich aus den

[1241] Siehe S. 83 ff.
[1242] Dies gilt, sofern der Dritte kein Vertragspartner des Providers des Kunden ist. Sollte der Dritte jedoch Vertragspartner des Providers des Kunden sein, dann gilt ebenso, dass die Zulässigkeit der Speicherung der E-Mail-Adresse in der Notwendigkeit begründet liegt, dass sie für den Aufbau weiterer Verbindungen erforderlich ist (vgl. S. 273).
[1243] Siehe zu den Bestandteilen einer E-Mail S. 272.

Regelungen der §§ 97, 99 oder 100 TKG nichts anderes ergibt.[1244] Diese Löschungspflicht bezieht sich auf den SMTP-Server, wobei für den POP3-Server, soweit der Provider also gleichzeitig Vertragspartner des Kommunikationspartners ist, die obigen Ausführungen im Verhältnis zwischen Provider und VPN-Auftraggeber entsprechend gelten.[1245]

Fraglich ist, ob hier eine Ausnahme von der Löschungspflicht gemäß § 96 Abs. 2 TKG in Betracht kommen könnte, sofern dem Provider der E-Mail-Kommunikationspartner nicht bekannt ist, da es sich insoweit um anonyme Daten für den Provider handelt. Diese Frage hat insbesondere aus dem Grunde Relevanz, da der Nutzer den Provider gemäß § 44 TKG auf Schadensersatz und Unterlassung in Anspruch nehmen kann.

Ob es sich bei der Zieladresse überhaupt um ein Datum handelt, mit welchem der Provider eine für ihn bestimmbare Person verknüpft, hängt davon ab, ob dem Provider, welcher dem VPN-Auftraggeber den E-Mail-Account eingerichtet hat, auch die Person der Zieladresse bekannt ist.[1246]

Ist der Empfänger ebenfalls Teilnehmer des Providers, bei welchem der VPN-Auftraggeber den E-Mail-Dienst beauftragt hat (was nicht zwangsläufig der Fall sein muss aber kann),[1247] so handelt es sich um ein personenbezogenes Datum, da dem Provider die Identität aufgrund dieses Zusatzwissens bekannt ist.[1248]

Der Provider muss demgemäß auf den technischen Systemen, welche für den Versand der E-Mail verantwortlich sind, für die Löschung Sorge tragen. Hierbei

---

[1244] Dies ist insoweit mit der Telefondatenerfassung vergleichbar, bei welcher die Belange des Angerufenen auch nicht außer Acht gelassen werden dürfen (Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 129. Auf S. 131 verweist Kleine-Voßbeck auch darauf, dass bei der Überwachung des E-Mail-Verkehrs weitergehende Kontrollmöglichkeiten als im Bereich der Telefonüberwachung denkbar sind, etwa durch Textanalyse anhand von Schlüsselbegriffen.). Siehe aber auch Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 98, die der Ansicht sind, dass aus Sicht des Angerufenen die Speicherung seiner Telefonnummer keine datenschutzrechtliche Relevanz zukommt.

[1245] Siehe S. 269 ff.

[1246] Siehe auch Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 49 und der Ausführung, dass die Domain Auskünfte über den Beruf des Nutzers geben kann. Sofern die Domain auf ein Unternehmen registriert ist, spricht alles dafür, dass der Nutzer für diese Firma tätig ist. Gehört sie zu einer Universität, so ist der Nutzer wahrscheinlich Student (Fröhle aaO).

[1247] Siehe auch Schema auf S. 63.

[1248] Vgl. zum Zusatzwissen insbesondere Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 33 ff.

handelt es sich regelmäßig um den SMTP-Server, den er als ein am Versand Beteiligter nutzt.[1249]

Ist der E-Mail-Empfänger kein Teilnehmer des Providers, bei dem auch der VPN-Auftraggeber den E-Mail-Dienst beauftragt hat, kommt es auf den Einzelfall an, inwieweit der Empfänger für den Provider anonym ist. In diesem Zusammenhang wird auf die Ausführungen zur Frage der Anonymisierung im zweiten Abschnitt dieser Arbeit verwiesen.[1250] Daten sind nur dann vollständig anonymisiert, sofern sämtliche Identifikationsmerkmale gelöscht werden. Gibt es auch nur eine weitere datenverarbeitende Stelle, der die Daten bekannt sind, kann keine Anonymisierung vorliegen. Hier geht insbesondere die Frage nach dem unverhältnismäßigen Aufwand fehl. Diese Frage kann sich nur stellen, wenn die datenverarbeitende Stelle ein Anonymisierungsverfahren entwickelt hat, welches „nahezu unmöglich" einen Datenrückschluss nicht mehr zulässt. Sofern aber die Identität durch den Wissensaustausch zweier datenverarbeitender Stellen in einfacher Weise hergestellt werden kann, liegt keine Anonymität vor.[1251] Damit sind ebenso faktisch anonyme Daten zu löschen.

Daher muss im Zweifel auch hier von einer Löschungsverpflichtung im Bezug auf Umschlag, Header und Inhalt der E-Mail oder der gegebenenfalls in einer Logdatei entstandenen Ziel-E-Mail-Adresse gemäß § 96 Abs. 2 TKG ausgegangen werden.[1252]

[1249] Siehe S. 269 ff.
[1250] Siehe S. 106 ff.
[1251] Siehe S. 215 ff. Siehe auch die Ausführungen von Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 51/52 zu den zahlreichen Verknüpfungsmöglichkeiten im Internet und der Möglichkeit, Nutzerdaten zusammen zu tragen, wobei er gleichzeitig die wachsenden Gefahren der Identitätsaufdeckung anspricht.
[1252] Siehe auch Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 37 mit dem Hinweis, dass es in der Praxis häufig unmöglich ist, zuverlässig abzuschätzen, ob zur Identifikation geeignetes Zusatzwissen vorliegt und daher im Zweifel vom Vorliegen des Personenbezugs auszugehen ist.

bb. Mitarbeiter

Die Pflicht zur Löschung gemäß § 96 Abs. 2 TKG bezüglich der in einer Logdatei entstehenden Daten der E-Mail-Verbindung sowie der aus Umschlag, Header und Inhaltsdaten bestehenden E-Mail gilt gleichermaßen im Rahmen der privaten Kommunikation der Nutzer, die Mitarbeiter des VPN-Auftraggebers sind.[1253]
Im Falle der ausschließlich dienstlichen Nutzung ist der Provider allein dem VPN-Auftraggeber zur Löschung der Daten gemäß § 96 Abs. 2 TKG verpflichtet.[1254] Bei einer „persönlichen dienstlichen“ Kommunikation (d.h. wenn in einer dienstlichen E-Mail ebenso private Details enthalten sind) besteht eine Löschungsverpflichtung gemäß § 96 Abs. 2 TKG sowohl gegenüber dem VPN-Auftraggeber als auch gegenüber dem Nutzer bzw. Mitarbeiter des VPN-Auftragnehmers. [1255]

Es ist allerdings fraglich, ob der Mitarbeiter dadurch in seinem Fernmeldegeheimnis gemäß § 88 TKG betroffen ist, sofern feststellbar ist, dass und zu welchem Zeitpunkt er „für“ den VPN-Auftraggeber kommuniziert hat.
Zu berücksichtigen ist zwar ebenso, dass der Nutzer dadurch in seinen personenbezogenen Daten betroffen ist, da in einer E-Mail-Adresse oftmals seiner vollständiger Name mit dem Unternehmensnamen verbunden ist. Daher ließe sich darauf schließen, dass der Nutzer bei dem Unternehmen angestellt ist.[1256]
Dies betrifft allerdings nicht einen Umstand, der vom TKG bzw. von den Löschungsverpflichtungen des § 96 TKG geschützt ist. Denn das TKG schützt allein Umstände, die sich auf Telekommunikationsvorgänge beziehen. Eine Löschungspflicht würde sich gemäß § 96 Abs. 2 TKG allein darauf beziehen, dass ein bestimmter Nutzer zu einem bestimmten Zeitpunkt an einem Telekommunikationsvorgang beteiligt war. Aber die Tatsache, dass ein

[1253] Siehe zur privaten Nutzung des E-Mail-Dienstes durch Arbeitnehmer auch Rosen, The unwanted gaze, The destruction of privacy in America, S. 54 ff. und 159 ff.
[1254] Siehe hierzu S. 269 ff.
[1255] Siehe zur Privatnutzung aus dienstlichem Anlass Däubler, Internet und Arbeitsrecht, Rn. 178. Sehe außerdem die Ausführungen in dem Personenverhältnis VPN-Auftraggeber/Nutzer auf S. 367 ff.
[1256] Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 49.

bestimmter Nutzer bei einem bestimmten Unternehmen beschäftigt ist, berührt nicht das Fernmeldegeheimnis.[1257]

Der Nutzer ist ebenso wenig in seinem Fernmeldegeheimnis gemäß § 88 TKG betroffen, wenn er ausschließlich dienstlich kommuniziert. Dies gilt ebenso unter Berücksichtigung der Tatsache, dass dieses nutzer- bzw. drittschützenden Charakter hat.[1258] In diesen Fällen kommuniziert er „für" den VPN-Auftraggeber und es handelt sich damit um die Kommunikation des VPN-Auftraggebers.
Die Löschungspflicht bezüglich der in einer Logdatei entstandenen E-Mail-Adresse des Nutzers und der damit zwangsläufig verbundenen Speicherung der Zuordnung des Namens des Nutzers mit dem Domain-Namen des VPN-Auftraggebers ergibt sich dementsprechend aus § 35 Abs. 2 BDSG.[1259] Durch die Speicherung dieser Zuordnung lässt sich auf die persönlichen und sachlichen Verhältnisse des Nutzers gemäß § 3 Abs. 1 BDSG schließen, so diese nur mit freiwilliger Einwilligung des Nutzers gemäß § 4a BDSG oder gemäß §§ 28 ff. BDSG zulässig ist. Letzteres kann in Betracht kommen, sofern der Provider den mit dem Domain-Namen des VPN-Auftraggebers verknüpften Namen des Nutzers für Authentifizierungszwecke auf den von ihm betriebenen Mailservern benötigt, und demzufolge auf diesen Systemen eine längerfristige Speicherung durch den Provider stattfinden muss.[1260]

Zu berücksichtigen ist ebenso, dass eine Löschung der Zuordnung zwischen Nutzername und Domain-Name des VPN-Auftraggebers auf anderen

---

[1257] Vgl. auch K. Lau in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 88 TKG Rn. 10 mit dem Hinweis, dass der Begriff der Telekommunikation die näheren Umstände der Telekommunikation schützt: Dies umfasst neben den Inhalten, die mit Hilfe der Telekommunikation übermittelt und bearbeitet werden auch die Frage, ob und wie die Telekommunikation stattgefunden hat, sowie wer daran teilgenommen hat.
[1258] Zur Gefährdung des Fernmeldegeheimnisses siehe S. 271. Zum nutzer- bzw. drittschützenden Charakter des Fernmeldegeheimnisses siehe Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 23; siehe zum persönlichen Schutzbereich des § 88 TKG Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 19; siehe ebenso Zerres in: Scheurle/Mayen, TKG-Kommentar, § 85 TKG Rn. 20. In diesem Sinne ebenso Klesczewski in: Berliner Kommentar zum TKG, § 88 TKG Rn. 10, der den personalen Anwendungsbereich zugunsten des „Anrufers" und des „Angerufenen" festlegt. Siehe außerdem die Ausführungen auf S. 436.
[1259] Vgl. zu den Einzelangaben auch Gola/Schomerus, BDSG, § 3 BDSG Rn. 3; Schulz in: Roßnagel, Recht der Multimedia-Dienste, § 1 TDDSG Rn. 28; Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 279. Zu den personenbezogenen Daten insgesamt S. 92 ff. in dieser Arbeit.
[1260] Siehe hierzu aber ebenso die datenschutzrechtlichen Ausführungen zum zwangsweisen Tunneling S. 284 ff.

technischen Systemen bzw. Datenträgern des Providers gemäß § 35 Abs. 2 BDSG zu erfolgen hat, sofern die Zuordnung für den Betrieb eines E-Mail-Accounts nicht mehr erforderlich ist. [1261] Dies kann insbesondere beim Ausscheiden des Mitarbeiters aus dem Unternehmen des VPN-Auftraggebers gelten.

Die sich aus § 93 S. 3 TKG ergebende Unterrichtungspflicht gegenüber den privaten Nutzern des E-Mail-Accounts kann der Provider dadurch erfüllen, dass er dem VPN-Auftraggeber die entsprechenden Informationen zur Weitergabe aushändigt. Ansonsten hat der Provider auch die Möglichkeit, diese Informationen auf seine Website zu stellen.

b. Technische Schutzmaßnahmen

Der Provider ist gemäß § 109 Abs. 2 TKG gegenüber den Nutzern dazu verpflichtet, angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen und zum Schutze gegen äußere Angriffe und Einwirkungen von Katastrophen der von ihm betriebenen öffentlichen[1262] Mailserver zu treffen, da diese Regelung nutzer- bzw. drittschützenden Charakter aufweist.[1263]

Diese Schutzmaßnahmen sowie die Verpflichtung zur Wahrung des Fernmeldegeheimnisses gemäß § 109 Abs. 1 TKG, § 88 TKG gegenüber den Mitarbeitern des VPN-Auftraggebers kann aber wiederum nur Geltung beanspruchen, soweit der Nutzer selbst Beteiligter der Kommunikation ist. Handelt es sich um ausschließlich berufliche Kommunikation, dann ist der Nutzer nicht betroffen bzw. allenfalls darin betroffen, dass Dritte gegebenenfalls möglich ist, seine Unternehmenszugehörigkeit festzustellen.[1264] Im Falle von privater Kommunikation ist der Provider jedoch verpflichtet, sowohl bezüglich des SMTP-Servers, mittels dem die von dem Nutzer verfassten E-Mails versendet werden, als auch bezüglich des POP3-Servers, mittels dem der

[1261] Siehe zur Erforderlichkeit S. 98.

[1262] Die Mailserver stehen regelmäßig einer Öffentlichkeit zur Verfügung gemäß § 3 Nr. 19 TKG a.F. zu Verfügung (siehe S. 277).

[1263] Siehe Büchner in: TKG-Kommentar (2. Auflage), § 40 TKG Rn. 5 zu § 87 Abs. 1 TKG a.F., wobei jedoch zu berücksichtigen ist, dass in § 109 Abs. 2 TKG Regelungen des § 87 Abs. 1 TKG a.F. enthalten sind. Siehe zu den Schutzzielen des § 109 TKG Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 25/26.

[1264] Siehe die gerade gemachten Ausführungen sowie Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 49.

Nutzer seine E-Mails abruft, die erforderlichen technischen Schutzmaßnahmen gemäß § 109 TKG zu treffen. [1265]

Etwas anderes ergibt sich jedoch im Hinblick auf den Empfänger der E-Mail, soweit dieser keine dem VPN-Auftraggeber allein zurechenbare Kommunikation führt, da die Pflichten der §§ 88, 109 TKG nicht nur und ausschließlich gegenüber einem Teilnehmer normiert sind, sondern sich an einen Diensteanbieter im Sinne des § 3 Nr. 6 TKG richten, der gegenüber Teilnehmern und Nutzern gleichermaßen verpflichtet ist, wie sich aus § 91 Abs. 1 TKG ergibt. Hier findet der nutzer- bzw. drittschützende Charakter des Fernmeldegeheimnisses gemäß § 88 TKG Anwendung,[1266] so dass der Provider gegenüber dem Empfänger der E-Mail zu den technischen Schutzmaßnahmen des § 109 TKG verpflichtet ist. Diese Verpflichtung besteht seitens des Providers und Betreibers des SMTP-Servers gegenüber dem Empfänger der E-Mail (als Nutzer). Im Hinblick auf den POP3-Server wird der E-Mail- Kommunikationspartner zum Teilnehmer gemäß § 3 Nr. 20 TKG, so dass dem Provider und Betreiber des POP3-Servers gegenüber dem E-Mail-Kommunikationspartner die gleichen Verpflichtungen obliegen wie die, die im Verhältnis zwischen VPN-Auftraggeber und Provider bereits festgestellt worden sind.[1267] Dementsprechend ist der Provider ebenso zur Unterrichtung über Verschlüsselungsmaßnahmen gemäß § 109 Abs. 1 TKG verpflichtet. Diese Pflicht besteht allerdings nicht unmittelbar gegenüber den Mitarbeitern des VPN-Auftraggebers, sofern diese ausschließlich beruflich kommunizieren. Hierbei ist allerdings zu berücksichtigen, dass der E-Mail-Kommunikationspartner vorrangig als Teilnehmer gemäß § 3 Nr. 20 TKG durch seinen Provider, der ihm den E-Mail-Account bereitstellt, über die Verschlüsselungsmaßnahmen gemäß § 109 Abs. 1 TKG zu unterrichten ist. Dies kann beispielsweise durch allgemein zugängliche Informationen auf der Website erfolgen.

[1265] Siehe S. 269 ff. (272), S. 62.
[1266] Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 23; siehe zum persönlichen Schutzbereich des § 88 TKG Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 19; siehe ebenso Zerres in: Scheurle/Mayen, TKG-Kommentar, § 85 TKG Rn. 20. In diesem Sinne ebenso Klesczewski in: Berliner Kommentar zum TKG, § 88 TKG Rn. 10, der den personalen Anwendungsbereich zugunsten des „Anrufers“ und des „Angerufenen“ festlegt. Siehe außerdem die Ausführungen und Verweise auf S. 436.
[1267] Siehe S. 269 ff.

c. Auskunfts- und Überwachungsmaßnahmen

Da das Fernmeldegeheimnis gemäß § 88 TKG nutzer- bzw. drittschützenden Charakter hat,[1268] kommen Überwachungsmaßnahmen nur unter den Voraussetzungen der TKÜV[1269] oder gemäß § 113 Abs. 1 S. 3 TKG und einer damit verbundene Anordnung nach § 100a StPO, § 100b Abs. 3 StPO, des § 2 Abs. 1 Satz 3 des G-10-Gesetzes, § 23a Abs. 1 S. 1 des Zollfahndungsdienstegesetzes oder nach Landesrecht in Betracht.[1270]

Dies gilt sowohl im Hinblick auf den E-Mail-Kommunikationspartner als auch im Hinblick auf den Nutzer im Unternehmen bzw. Mitarbeiter des VPN-Auftraggebers. Letzterer ist allerdings nur in seinem Fernmeldegeheimnis gemäß § 88 TKG oder personenbezogenen Daten betroffen, sofern er privat kommuniziert. Diesbezüglich wird auf die obigen Ausführungen verwiesen.[1271]

[1268] Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 23; siehe zum persönlichen Schutzbereich des § 88 TKG Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 19; siehe ebenso Zerres in: Scheurle/Mayen, TKG-Kommentar, § 85 TKG Rn. 20. In diesem Sinne ebenso Klesczewski in: Berliner Kommentar zum TKG, § 88 TKG Rn. 10. Siehe außerdem S. 436.
[1269] Vgl. hierzu S. 263.
[1270] Siehe hierzu auch die Ausführungen in der Einführung S. 13. Siehe zur E-Mail-Überwachung ebenso Ullrich in: Holznagel/Nelles/Sokol, TKÜV, S. 20.
[1271] Vgl. S. 292 ff. Siehe außerdem S. 261 ff.

C. VPN-Auftraggeber - Nutzer

Entsprechend der obigen Ausführungen fällt auch in diesem Personenverhältnis sowohl der derjenige unter den Begriff des Nutzers, dem der VPN-Auftraggeber das VPN oder den Zusatzdienst E-Mail zur Nutzung bereitstellt, insbesondere also dessen Mitarbeiter.[1272] Als Nutzer des erbrachten Dienstes wird in dieser Arbeit darüber hinaus ebenso derjenige betrachtet, der auf der „gegenüberliegenden Kommunikationsseite“ steht. Damit ist der Inhaber der Ziel-Domain-Adresse bzw. der Website-Betreiber sowie der E-Mail-Empfänger gemeint.

Die Verwendung des Nutzerbegriffs für Kommunikationspartner ist gerechtfertigt, da diese sich insoweit selbständig und willentlich in die allgemeine Kommunikation per Internet durch Bereithaltung eines E-Mail-Accounts oder einer Website als Beteiligte einbringen. Dieses Verständnis entspricht ebenso der dieser Arbeit zugrunde gelegten Definition, dass es sich bei einem Online-Dienst (abstrakt) um eine wirtschaftliche Tätigkeit handelt, die im Internet erbracht wird. Eine solche Definition ermöglicht die abstrakte Sichtweise (beispielsweise) einer Internetverbindung in dem Sinne, dass an dieser mehrere Anbieter und Nutzer aktiv beteiligt sein können.

I. Rechtliche Einordnung der Dienste im VPN

Entsprechend der Aufbaulogik dieser Arbeit erfolgt wiederum zunächst eine rechtliche Einordnung der Dienste im VPN als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG oder Teledienst gemäß § 2 Abs. 1 TDG. Bei den Diensten handelt es sich im Einzelnen um die Bereitstellung einer Internetverbindung bzw. eines Internetzugangs, der VPN-Kommunikation sowie des Zusatzdienstes E-Mail.[1273] Im Anschluss daran erfolgt die datenschutzrechtliche Prüfung. [1274]

[1272] Siehe S. 83 und S. 279 ff
[1273] Vgl. S. 120 ff. sowie S. 279 ff.
[1274] Vgl. S. 162 ff. sowie S. 280 ff.

1. Internetverbindung[1275]

Ursprünglich war zwar umstritten, ob Diensteanbieter ohne Gewinnerzielungsabsicht überhaupt Telekommunikationsdienste anbieten konnten. Denn einerseits deutete das Tatbestandsmerkmal „geschäftsmäßig“ entsprechend der Definition in § 3 Nr. 5 TKG a.F. darauf hin, dass es auf die Gewinnerzielungsabsicht nicht ankommt. Andererseits war dem Begriff der „Telekommunikationsdienstleistungen“ gemäß § 2 Nr. 6 TDSV 1996 die Gewerblichkeit immanent, so dass der Begriff „geschäftsmäßig“ als überflüssig und irreführend eingestuft worden ist, und als Diensteanbieter vielmehr nur diejenigen angesehen wurden, die Telekommunikationsdienstleistungen mit Gewinnerzielungsabsicht angeboten haben.[1276]
Danach konnte ein Arbeitgeber im eigentlichen Sinne kein Diensteanbieter von Telekommunikationsdienst(-leistung)en sein, da er im Verhältnis zu seinen Arbeitnehmern bzw. Nutzern nicht mit Gewinnerzielungsabsicht handelt.[1277]
Dies hat sich bereits durch die neue Fassung des TDSV geändert, da gemäß der amtlichen Begründung zu dieser Verordnung[1278] alle Diensteanbieter erfasst sind, die im Sinne des § 3 Nr. 5 TKG a.F. in Verbindung mit § 3 Nr. 19 TKG a.F. mit oder ohne Gewinnerzielungsabsicht für beliebige natürliche oder juristische Personen, einschließlich Teilnehmer geschlossener Benutzergruppen, Telekommunikationsdienste nachhaltig anbieten.
Somit können nunmehr auch Arbeitgeber generell als Anbieter von Telekommunikationsdiensten gelten, insbesondere da nun in § 3 Nr. 24 TKG nicht mehr vorausgesetzt ist, anders als in § 3 Nr. 18 TKG a.F., dass ein Telekommunikationsdienst gewerblich erbracht wird.[1279]

[1275] Anzumerken ist, dass als Nutzer hier regelmäßig allein die Mitarbeiter des VPN-Auftraggebers in Betracht kommen, da externe Nutzer, wie etwa Lieferanten, regelmäßig ihren eigenen Access-Provider beauftragt haben.
[1276] Büchner in: TKG-Kommentar (2. Auflage), § 2 TDSV (Anh § 89 TKG) Rn. 3.
[1277] Siehe auch Gola/Klug, Grundzüge des Datenschutzrechts, S. 189/190.
[1278] Amtliche Begründung zur Telekommunikations-Datenschutzverordnung (TDSV) vom 18. Dezember 2000 (BGBl. I S. 1740), S. 1.
[1279] Vgl. auch Mengel, BB 2004, 2014, 2017; Heidrich/Tschoepe, MMR 2004, 75, 76. Siehe zur Einstufung eines Arbeitgebers als Diensteanbieter gemäß § 3 Nr. 6 TKG auch Schmidl, DuD 2005, S. 267, 269.

Teilweise wird der Arbeitgeber durch die Bereitstellung des Internetzugangs zwar als Telediensteanbieter im Sinne von § 2 Abs. 2 Nr. 3 TDG eingestuft.[1280] Es wurde jedoch bereits festgestellt, dass es sich allgemein bei der Bereitstellung des Internetzugangs um einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG handelt.[1281] Hieran ändert auch ein bestehendes Arbeitsverhältnis nichts. Denn die Einordnung von Access-Providing als Teledienst ist in dieser Arbeit im Wesentlichen mit der Begründung abgelehnt worden, dass die Möglichkeit der Datenübertragung im Vordergrund steht, ohne dass es hier auf die konkreten Inhalte ankommt.[1282]
Daher ist kein Grund ersichtlich, warum nun der Arbeitgeber als Telediensteanbieter eingestuft werden sollte. Der Arbeitgeber ist im Verhältnis zu seinen Mitarbeitern demgemäß Anbieter eines Telekommunikationsdienstes gemäß § 3 Nr. 24 TKG, da er ebenfalls nur die technischen Voraussetzungen zur Datenübertragung zur Verfügung stellt, und zwar anwendungsdiensteunabhängig.[1283]

2. VPN-Kommunikation

Neben der Bereitstellung der Internetverbindung stellt die „eigentliche" VPN-Kommunikation eine weitere Dienstleistung eines VPN dar.[1284] Auch hier ist im Verhältnis zwischen Nutzer und VPN-Aufraggeber zu untersuchen, ob diese VPN-Kommunikation die Bereitstellung eines Telekommunikationsdienstes gemäß § 3 Nr. 24 TKG oder eines Teledienstes gemäß § 2 Abs. 1 TDG beinhaltet. Dies ist Gegenstand der nachfolgenden Untersuchung.

[1280] Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 80; Globig/Eiermann, DuD 1998, 513, 516; Gola, NJW 1999, 3753, 3755. Post-Ortmann, RDV 1999, 102, 105 nimmt einen Teledienst gemäß § 2 Abs. 2 Nr. 3 TDG nur für den Fall an, wenn der Arbeitgeber seinen Mitarbeitern den Internetzugang zu einer von der dienstlichen Nutzung abgrenzbaren privaten Nutzung überlässt, da anderenfalls (im Falle einer dienstlichen Nutzung) mangels Angebot und Nachfrage bzw. einer freiwilligen Inanspruchnahme die Regelungen des BDSG einschlägig seien. Vgl. auch Müller, RDV 1998, 205, 210, der der Ansicht ist, dass das TKG nicht den Schutz der individuellen Kommunikation per E-Mail oder auf anderem Wege zwischen Sender und Empfänger, sprich Arbeitgeber und Arbeitnehmer oder Drittem zum Gegenstand hat, sondern dass vielmehr die Regelungen des TKG der grundsätzlichen Ausgestaltung der Telekommunikationsnetze als Infrastrukturleistung dienen.
[1281] Siehe außerdem Gola, MMR 1999, 321, 328 zu der Frage, ob es sich generell um ein Angebot-Nutzer-Verhältnis handelt.
[1282] Siehe S. 122 ff.
[1283] Siehe S. 126. Ebenso Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 41 (Ein Arbeitgeber, der seinen Arbeitnehmern die Nutzung des unternehmenseigenen Internetanschlusses erlaubt, erbringt einen Telekommunikationsdienst).
[1284] Siehe S. 120.

a. Internet-Dienst[1285]

aa. Tunneling-Protokolle

Fraglich ist, ob der VPN-Auftraggeber[1286] allein durch die Bereitstellung der Daten mittels Tunneling-Technik einen Teledienst im Sinne von § 2 Abs. 2 Nr. 3 TDG anbieten könnte.[1287] Denn so wird beispielsweise für den Internet-Dienst[1288] ftp (file transfer protocol), ein Internet-Protokoll, welches die Übertragung von Daten anstatt http[1289] über das Internet ermöglicht,[1290] vertreten, dass es sich aufgrund des Client-Server-Prinzips[1291] entweder um einen Teledienst handeln soll, da ihm die redaktionelle Gestaltung fehlt, oder aber aus dem Grunde einen Mediendienst darstellen, da er an eine Öffentlichkeit gerichtet ist.[1292]

Diese Sichtweise könnte auf Tunneling-Techniken entsprechend anwendbar sein, da diese ebenso den Datentransport bzw. die Übertragung von Daten über das Internet mittels des Client-Server-Prinzips ermöglichen, da ein Client auf den Gateway bzw. beim Software-VPN auf den Rechner, auf dem die entsprechende VPN-Technik installiert ist, zugreift.
Jedes Tunneling-Protokoll ist als Verfahren zum Transport von Datenpaketen über andere Netze allgemein anerkannt.[1293] Konsequenz hieraus wäre, dass ohne weitere Prüfung ein Teledienst beim Datenaustausch zwischen Firmenzentrale und Nutzer bzw. zwischen verschiedenen Nutzern untereinander oder beim Datenabruf eines Nutzers anzunehmen ist.

[1285] Zur Abgrenzung sei kurz angemerkt, dass es hier nicht auf ein Angebot im Sinne von § 2 Abs. 2 Nr. 3 TDG ankommt (Angebot zur Nutzung des Internet), sondern allein auf die bereitgehaltenen Daten. Denn das Angebot zur Nutzung des Internet wurde bereits oben auf S. 122 ff. diskutiert und beinhaltet die Bereitstellung des VPN (an sich) mittels Tunneling-Technik und Internetzugang.
[1286] Nutzer können sowohl Mitarbeiter als auch Externe sein.
[1287] Hierzu ist entsprechende Software sowohl auf dem Rechner des Nutzers als auch auf dem Rechner (zum Software-VPN siehe S. 53 ff.) oder Gateway (zum Gateway-VPN siehe S. 44 ff.) des VPN-Auftraggebers erforderlich.
[1288] Siehe zum Internet-Dienst S. 75 ff.
[1289] Siehe zum Begriff „http“ S. 23.
[1290] Zum Übertragungsprotokoll „ftp“ siehe S. 23, insbesondere Fn. 82.
[1291] Siehe hierzu S. 43.
[1292] Spindler in: Roßnagel, Recht der Multimedia-Dienste, § 2 TDG Rn. 82 ff.; Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 83; vgl. zur Einordnung als Mediendienst Holznagel/Kibele in: Hoeren/Sieber, Teil 5 Rn. 68.
[1293] Böhmer, Virtual Private Networks (2. Auflage), S. 206.

Hiergegen gibt es jedoch hauptsächlich die folgenden zwei Argumente, die sich aus dem Vergleich mit anderen Nutzungsvorgängen im Internet (zwischen einem Anbieter und einem Nutzer) ergeben.
Zum einen kann die gerade genannte Auffassung, dass stets bei einem Angebot, das auf dem Client-Server-Prinzip basiert und dem die redaktionelle Gestaltung fehlt, ein Teledienst gegeben ist, nicht überzeugen.[1294]
Dass dies in dieser Allgemeinheit nicht richtig sein kann, zeigt bereits, dass anderenfalls im Zusammenhang mit im Internet erbrachten Dienstleistungen von vorneherein nicht mehr über Telekommunikationsdienste diskutiert werden müsste. Es würde vielmehr zwischen einem Anbieter und einem Nutzer in allen Fällen das TDG Anwendung finden, da bei jeder Internetnutzung ruft regelmäßig ein Client einen Server an, um dessen Dienst in Anspruch zu nehmen, und zwar sowohl beim Internetzugang durch Anruf oder Inanspruchnahme des jeweiligen Internetzugangsknotens als auch bei Aufruf einer Website.
Zum anderen berücksichtigt eine solche Sichtweise außerdem nicht die unterschiedlichen Möglichkeiten, die mittels Protokollen bereitgestellt werden können. Denn so können die inhaltlichen Angebote oder Informationen, die der Betreiber des Servers mittels ftp zum Abruf bereithält letztendlich Teledienste darstellen, wobei ein Mediendienst in Betracht kommt,[1295] sofern das „dahinter stehende“ Angebot redaktionell gestaltet ist.[1296] Denn diese Inhalte bilden das

[1294] Siehe auch Kröger/Moos, ZUM 1997, 462, 466 ff.; insbesondere S. 467; Kröger/Moos, AfP 1997, 675, 679, die darauf verweisen, dass alle Internet-Dienste aufgrund des Client-Server-Prinzips als Tele- oder Mediendienste einzustufen sind.
[1295] Die inhaltliche Abgrenzung zwischen Tele- und Mediendiensten ist aufgrund der Beispielkataloge in § 2 Abs. 2 TDG und § 2 Abs. 2 MDStV, die viele Überschneidungen enthalten, umstritten (siehe hierzu auch S. 67, insbesondere Fn. 295/296in dieser Arbeit). Vgl. hierzu: Ladeur, ZUM 1997, 372, 382; Waldenberger, MMR 1998, 124, 124; Kröger/Moos, AfP 1997, 675 ff.; Roßnagel, NVwZ 1998, 1, 3; Hochstein, NJW 1997, 2977, 2980; Pichler, MMR 1998, 79, 80 ff.; v.Bonin/Köster, ZUM 1997, 462, 466; Gounalakis, NJW 1997, 2993, 2995; Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 25; Moritz in: Büllesbach, Datenverkehr ohne Datenschutz ?, S. 98/99; siehe auch Engel, MMR-Beilage 4/2003, 1, 14 ff.
[1296] Eberle in: Eberle/Rudolf/Wasserburg, Kapitel I Rn. 68; Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2983; Waldenberger, MMR 1998, 124, 125; Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 76/77; Eichhorn, Internet-Recht, S. 32 ff.; Pankoke, Von der Presse- zur Providerhaftung, S. 32 ff., der eine Abgrenzung zwischen individueller Nutzung und redaktioneller Gestaltung zur Meinungsbildung für die Allgemeinheit vornimmt; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 77; vgl. außerdem Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 75 ff., der die Individualkommunikation (Teledienst) und redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit (Mediendienst) im Sinne der gesetzlichen Fassung gemäß § 2 Abs. 1 MDStV i.V.m. §§ 2 Abs. 4 Nr. 3, Abs. 2 Nr. 2 TDG als Abgrenzungskriterien nimmt und eine Abgrenzung zwischen Telediensten und Mediendiensten anhand des Beispiels eines Werbebanners auf Internet-Seiten vornimmt; siehe zur redaktionellen Gestaltung außerdem

für einen Tele- oder Mediendienst erforderliche konkrete Informationsangebot des Providers an den Nutzer.[1297] Daher kann gleichermaßen ein Telekommunikationsdienst in Frage kommen, sofern der Provider ftp für den reinen Datentransfer zur Verfügung stellt.[1298] So wird ein ftp-Zugang regelmäßig von einem Anbieter im Rahmen eines Website-Hosting-Vertrages angeboten, damit seine Kunde ihre Daten auf der (gehosteten) Website eigenständig zu verändern und zu pflegen.[1299]

Diesbezüglich wäre es nicht folgerichtig, einen Teledienst zugrunde zu legen, da der jeweilige Anbieter selbst kein inhaltliches Angebot zur Verfügung stellt, sondern nur die Möglichkeit einer Datenübertragung. Es liegt hier keine Abrufmöglichkeit von Informationen durch den Nutzer vor, wie es aber für die Anwendung des TDG nach § 2 Abs. 2 erforderlich ist,[1300] sondern es geht hier vorrangig darum, dass der Server eines Anbieters funktionstüchtig ist, also um die Verständigung zwischen Sender und Empfänger sowie dem Transport von Inhalten. Der transportierte Inhalt selbst ist hier nicht entscheidend.[1301] Der jeweilige Anbieter hat vielmehr lediglich dafür Sorge zu tragen, dass sein Server an das Internet angeschlossen ist, um den Datentransport sicher zu stellen.[1302] Der bereitgehaltene Server ist dementsprechend eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG, da er ein System darstellt, welches als Nachrichten identifizierbare elektromagnetische oder optische Signale empfangen und kontrollieren kann.[1303] Der Anbieter selbst bietet eine Transportdienstleistung an, da hier der Empfang der Nachrichten im

---

Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 26; Gounalakis/Rhode, CR 1998, 487, 490; v.Heyl, ZUM 1998, 115, 118.

[1297] Vgl. Beck-IuKDG-Tettenborn, § 2 TDG Rn. 40; vgl. zur Notwendigkeit der Abrufbarkeit auch Koch, CR 1997, 193, 199. Institutionen, wie Universitäten, bieten ihren Angehörigen oftmals den Zugriff auf ihr eigenes Netz und Angebote mittels ftp an. Derjenige, der lediglich die Datenübertragung mittels ftp durch Bereitstellung der technischen Voraussetzungen ermöglicht, bietet selbst aber keine Inhalte an (siehe auch Fn. 82).

[1298] Vgl. auch Schuppert, CR 2000, 227, 230.

[1299] Vgl. Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil V Rn. 4/22/72 sowie Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil V Rn. 32 ff..

[1300] Vgl. auch Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 42, der am Beispiel des Access-Providers darauf hinweist, dass bei einem Teledienst zusätzlich erforderlich ist, dass Inhalte unmittelbar zur Verfügung gestellt werden. Siehe außerdem Koch, CR 1997, 193, 199; Beck-IuKDG-Tettenborn, § 2 TDG Rn. 40.

[1301] Vgl. auch Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 75, der Telekommunikation als jedweden Vorgang begreift, welcher ohne nach Inhalt zu unterscheiden und anwendungsdiensteunabhängig ausschließlich die Übertragung der Nachrichten und die Verständigung zwischen Sender und Empfänger regelt (siehe auch S. 126).

[1302] Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil V Rn. 40 ff.; Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil V Rn. 32 ff.

[1303] Zum weiten Begriffsverständnis einer Telekommunikationsanlage siehe Krader, Das neue Telekommunikationsrecht in der Praxis, S. 117 sowie S. 114 in dieser Arbeit.

Vordergrund steht.[1304] Dementsprechend ist er auch Diensteanbieter gemäß § 3 Nr. 6, 24 TKG.
Es fehlt damit insgesamt an einer inhaltlichen Komponente eines bereitgestellten Angebots, da ebenso wenig ein Zugang zu (fremden) Inhalten gemäß § 2 Abs. 2 Nr. 3 TDG vermittelt wird.[1305]

Diese allgemeinen Überlegungen bezüglich der Verwendung von Protokollen in Anbieter-Nutzer-Verhältnissen des Internet müssen entsprechend für die Tunneling-Protokolle gelten. Bei einem VPN kommt neben der Bereitstellung von Daten (zum Abruf) auf den Servern der Firmenzentrale ebenso in Betracht, dass die Nutzer eigenständig Daten auf die Server der Firmenzentrale übertragen können. So können beispielsweise mittels der im technischen Teil dargestellten Protokollen L2TP oder IPSec durch einen seitens des Nutzers initiierten Übertragungsvorgang Daten übermittelt werden.

Hieran wird deutlich, dass ftp sowie die Tunneling-Techniken unterschiedliche Zwecke erfüllen und Verwendungsmöglichkeiten haben können und daher nicht pauschal als Teledienste eingestuft werden sollten.

bb. OSI-Schichtenmodell

Etwas anderes ergibt sich auch nicht aus dem OSI-Schichtenmodell.[1306] Zwar sind Tunneling-Protokolle in der Transportschicht angesiedelt,[1307] aber dennoch sollte nicht generell den verschiedenen Schichten des OSI-Schichtenmodells eine Bedeutung für die Einordnung als Telekommunikations- oder Teledienst zugemessen werden, sondern stets auf das „dahinter liegende“ Angebot, sprich das Informationsangebot des (Content[1308])-Providers abgestellt werden.

[1304] Vgl. Schuster in: TKG-Kommentar (2. Auflage), § 3 TKG Rn. 21a; vgl. auch Wittern/Schuster in: TKG-Kommentar (3. Auflage), § 3 TKG Rn. 48.
[1305] Zwar erfolgt hier ein konkretes Angebot an einen bestimmten, angesprochenen Nutzer (vgl. Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 80) im Sinne einer Hilfe (Bundestag-Drucksache 13/7385, S. 19) zur Nutzung des ftp-Zugangs oder der Tunneling-Technik. Aber wie bereits auf S. 135 ff. ausgeführt fallen hierunter Angebote, bei denen dennoch die inhaltliche Komponente im Vordergrund steht (unter anderem Navigationshilfen oder Suchmaschinen). Siehe außerdem zur Ablehnung der Datenverschlüsselung als Teledienst S. 265 ff.
[1306] Siehe zum OSI-Schichtenmodell S. 22.
[1307] Siehe S. 34.
[1308] Siehe zu diesem Begriff S. 80.

Der Auffassung, dass eine Einteilung der Dienste anhand des OSI-Schichtenmodells vorgenommen werden sollte, wonach der Telekommunikationsvorgang die Schichten 1-5 des OSI-Modells abbildet und das TDG nur für die Schichten 6 und 7 gelten soll,[1309] ist daher nicht zu folgen.[1310] Denn das OSI-Schichtenmodell ist nichts anderes als ein Modell für die Struktur des Internet.[1311] Die Dienste, die dort angesiedelt sind, sind im Sinne der obigen Definition Internet-Dienste, wobei es sich um Kommunikationsstrukturen[1312] handelt.

Die Einordnung als Tele- oder Telekommunikationsdienst ausschließlich anhand des OSI-Schichtenmodells führt beispielsweise bei ftp und dem Tunneling-Protokoll IPSec zu unklaren Lösungen. Denn aufgrund der Tatsache, dass sowohl der ftp-Vorgang als auch die IPSec-Verschlüsselung „IKE“ auf einer der oberen Schichten des OSI-Schichtenmodells abläuft,[1313] käme man zur Einordnung als Teledienst gemäß § 2 Abs. 1 TDG, obwohl oben festgestellt worden ist, dass es sich diesbezüglich ebenso um einen Telekommunikationsdienst handeln kann.

Auch bei Verschlüsselungstechniken birgt die Einordnung als Tele- oder Telekommunikationsdienst anhand des OSI-Schichtenmodells Ungereimtheiten in sich, da Verschlüsselung grundsätzlich auf jeder Schicht möglich ist.[1314] Demzufolge wäre ein technischer Vorgang (Verschlüsselung) unterschiedlich zu beurteilen, je nachdem ob dieser Vorgang etwa auf Schicht 2 oder, wie bei IPSec, Schicht 5 erfolgt. Dies erscheint nicht zweckgerecht.

Diese Beispiele zeigen, dass es sich empfiehlt, eine Verknüpfung stets vom konkreten Dienst ausgehend auf die jeweilige Schicht des OSI-Schichtenmodells vorzunehmen und nicht umgekehrt.[1315] Denn zuerst muss

[1309] Vgl. etwa Pankoke, Von der Presse- zur Providerhaftung, S. 43.
[1310] Vgl. Pankoke, Von der Presse- zur Providerhaftung, S. 41 ff.; Hoeren, MMR 1998, 1, 4; Tettenborn, MMR 1999, 516, 518; Koenig/Neumann, K&R 1999, 144, 147/149; Sieber in: Hoeren/Sieber, Teil 19 Rn. 245; Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 86/87.
[1311] Tanenbaum, Computernetzwerke, S. 658.
[1312] Vgl. Janssen, Die Regulierung abweichenden Verhaltens im Internet, S. 83 ff.
[1313] Siehe auch Davis, IPSec, S. 43.
[1314] Siehe Lipp, VPN, S. 91.
[1315] Vgl. Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 89; Pankoke, Von der Presse- zur Providerhaftung, S. 42, der darauf verweist, dass es „doppelfunktionale“ Dienstleistungen gibt, die sowohl vom TKG als auch gleichzeitig vom TDG erfasst werden können, so dass TDG und TKG, insbesondere bezogen auf die Haftungsfreistellung nach § 5 Abs. 3 S. 1 TDG a.F., parallel anzuwenden sind. Vorliegend konzentriert sich die Fragestellung jedoch nicht darauf, ob es bei der Einordnung ein „Sowohl-als-auch“ gibt, sondern ob es überhaupt zweckmäßig und richtig ist, von der einzelnen Schicht

geprüft werden, ob überhaupt ein Telekommunikations- oder Teledienst vorliegt, oder ob es sich nicht lediglich um ein technisches Werkzeug des Internet, sprich einen Internet-Dienst handelt. Erst im Anschluss daran ist zu untersuchen, welches konkrete Leistungsangebot der jeweilige Anbieter unterhält, und zwar ob dies vorrangig den technischen Übertragungsvorgang erfasst oder vielmehr inhaltsbezogen ist,[1316] wobei, wie den gerade gemachten Ausführungen zu entnehmen ist, der jeweilige Verwendungszusammenhang eine entscheidende Rolle spielt.
Anhand des hier untersuchten Personenverhältnisses „Auftraggeber/Nutzer" eines VPN kann also die Feststellung getroffen werden, dass die Anwendbarkeit des OSI-Schichtenmodells für die Einordnung eines Dienstes als Telekommunikationsdienst oder Teledienst nicht zielführend ist und dem OSI-Schichtenmodell keine Allgemeingültigkeit im Hinblick auf die Einordnung von Diensten als Telekommunikationsdienst oder Teledienst entnommen werden kann.

b. Online-Dienst

Die Bedeutung der unterschiedlichen Einsatzmöglichkeiten der Tunneling-Protokolle zeigt sich bei einem VPN ebenso unter Berücksichtigung der folgenden Ausführungen.

aa. Teledienst

Die interne Kommunikation eines VPN kann dadurch stattfinden, dass die Nutzer auf den (seitens des VPN-Auftraggebers bereitgestellten) Server der Firmenzentrale zugreifen und von dort Daten bzw. Informationen auf ihren eigenen Rechner herunterladen,[1317] oder aber im Wege des Application Service Providing[1318] bereit gestellt bekommen.

---

auf den Dienst zu schließen, ohne die Frage der doppelfunktionalen Dienstleistungen in den Vordergrund zu stellen.

[1316] Vgl. auch S. 122 ff., insbesondere S. 126.

[1317] Vgl. auch die Bildbeispiele S. 2/44 ff.

[1318] Vgl. zu Application Service Providing die Ausführungen auf S. 74/81 ff. Siehe ebenso Lipp, VPN, S. 399 zur Integration von Application Service Providing in ein VPN.

Zwar steht beim Bereithalten von Inhalten seitens des VPN-Auftraggebers, und zwar unabhängig davon, ob durch ein Abrufverfahren mittels Download oder mittels Application Service Providing,[1319] der Inhaltsbezug gemäß § 3 Nr. 1 TDG im Vordergrund, da der VPN-Auftraggeber eigene Informationen zur Nutzung bereit hält.[1320].

Jedoch wird im Rahmen einer geschlossenen Benutzergruppe, die Auffassung vertreten, dass es sich nicht um ein Angebot-Nutzer-Verhältnis handelt, wie es aber für die Anwendung des TDG erforderlich ist,[1321] sondern um ein Nutzer-Nutzer-Verhältnis.[1322]

Hierbei ist allerdings zum einen zu beachten, dass der Begriff der geschlossenen Benutzergruppe dem TKG entstammt.[1323]

Zum anderen ergibt sich ebenso aus dem Umkehrschluss des § 1 Abs. 1 S. 2 Nr. 1 und Nr. 2 TDDSG,[1324] dass die Einordnung des VPN-Auftraggebers bzw. Arbeitgebers als Telediensteanbieter im Sinne von § 2 Abs. 2 Nr. 1 TDG grundsätzlich in Betracht kommt, sofern dieser auf seinem Server Informationen

---

[1319] Vgl. Röhrborn/Sinhart CR 2001, 69, 74, die eine Einordnung von Application Service Providing als Teledienst vornehmen. A.A. jedoch Bettinger/Scheffelt, CR 2001, 729, 732, die Application Service Providing als Telekommunikationsdienst einordnen. Ohne diese Frage in dieser Arbeit umfassend behandeln zu wollen, erscheint eine Einordnung als Teledienst folgerichtig, da es im Verhältnis zwischen Nutzer und VPN-Auftraggeber vordergründig um die Bereitstellung von Inhalten geht, so dass der Dienst gerade nicht anwendungsdiensteunabhängig erbracht wird. Für eine Einordnung als Telekommunikationsdienst könnte allenfalls das Argument sprechen, dass es Nutzer und VPN-Auftraggeber nur darauf ankommt, dass die Übertragung im Wege eines Fernzugriffs funktioniert, unabhängig von den bereitgestellten Daten. Dennoch legt § 2 Abs.1 TDG eindeutig fest, dass ein Teledienst dann in Betracht kommt, sofern Daten, Bilder, etc. individuell genutzt werden können. Diese individuelle Nutzungsmöglichkeit bietet Application Service Providing.

[1320] In Einzelfall könnte auch ein Mediendienst gemäß § 2 Abs. 1 MDStV in Frage kommen, sofern die redaktionelle Gestaltung im Vordergrund steht, was jedoch bei einem firmenintern genutzten VPN nur ausnahmsweise in Betracht kommen dürfte (siehe zur Abgrenzung zwischen Tele- und Mediendienst die obigen S. 306 Fn. 1295/1296 mit weiteren Verweisen auf S. 67, insbesondere Fn. 295/296i n dieser Arbeit).

[1321] Siehe auch die Ausführungen zu Routern auf S. 143 ff. Es ist im Übrigen auch richtig im Rahmen eines Teledienstes ein Angebot-Nutzer-Verhältnis zu verlangen, da dies nicht nur dem Wortlaut des § 2 TDG entspricht, sondern sich aus den Regelungen des TDG ergibt, Nutzer von Diensten, beispielsweise durch Regelungen wie § 6 TDG zu schützen. Besonderer Schutzvorschriften bedarf es jedoch dann nicht, wenn die Nutzer gleichberechtigt auf einer Ebene stehen bzw. kommunizieren.

[1322] Vgl. Gola/Müthlein, TDG/TDDSG, § 2 TDG S. 88; Tettenborn, MMR 1999, 516/518.

[1323] Hierbei sind im Rahmen einzelner datenschutzrechtlicher Regelungen des TKG für Anbieter geschlossener Benutzergruppen Erleichterungen geschaffen worden, siehe auch S. 184.

[1324] § 1 Abs. 1 S. 2 TDDSG regelt, dass die datenschutzrechtlichen Regelungen des TDDSG weder bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Dienst- und Arbeitsverhältnis gelten, soweit die Nutzung der Teledienste zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt (Nr. 1), noch bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten innerhalb von oder zwischen Unternehmen oder öffentlichen Stellen, soweit die Nutzung der Teledienste zur ausschließlichen Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

zum Abruf bereitstellt, und zwar auch dann, sofern die Informationen im Verhältnis zu seinen Mitarbeitern zu betriebsinternen, im Verhältnis zu Externen, wie etwa Lieferanten, zu geschäftsinternen Zwecken zur Verfügung stehen.[1325] In diesem Falle liegt ein Teledienst vor, wobei allerdings das TDDSG keine Anwendung findet.[1326]
Dies bedeutet, dass ebenso ein Teledienst gemäß § 2 Abs. 2 Nr. 1 TDG vorliegt, wenn der VPN-Auftraggeber mittels eines Software-VPN die Möglichkeit schafft, dass die Nutzer untereinander in gleichberechtigter Form Inhalte austauschen können und es sich insoweit um ein Nutzer-Nutzer-Verhältnis handelt.[1327] Denn in diesem Falle steht zwischen den jeweiligen Nutzern gemäß § 2 Abs. 2 Nr. 1 die Individualkommunikation im Vordergrund, so dass ein Nutzer im Verhältnis zu einem anderen Nutzer einen Teledienstanbieter gemäß § 2 Abs. 1 Nr. 1 TDG darstellt.[1328]

bb. Telekommunikationsdienst

Ein VPN kann zwischen Nutzer und VPN-Auftraggeber darüber hinaus dazu genutzt werden, um Daten des Nutzers auf den Server der Firmenzentrale selbständig zu übertragen und dort zu speichern.
Dies ist sowohl mit dem oben genannten ftp-Service vergleichbar, der einem Nutzer die Möglichkeit bietet, eigenständig Daten auf einem Server zu speichern,[1329] als auch mit einem Online-Backup-Verfahren[1330], sofern der VPN-Auftraggeber beispielsweise Tochterunternehmen, Zweigstellen oder Telearbeitern die Möglichkeit bietet, Daten auf dem Unternehmensserver zu speichern. Hierbei steht nicht der Inhaltsbezug im Vordergrund, sondern die Transportfunktion, da anwendungsdiensteunabhängig[1331] lediglich die Datenübertragung zum Server in der Firmenzentrale ermöglicht werden soll. Bei

[1325] Vgl. auch Gola, MMR 1999, 321, 328.
[1326] Vgl. auch Erwägungsgrund 18 der E-Commerce-Richtlinie, in dem geregelt ist, dass die Verwendung elektronischer Post oder gleichwertiger individueller Kommunikation zum Beispiel durch natürliche Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit, kein Dienst der Informationsgesellschaft ist (zur E-Commerce-Richtlinie siehe im Übrigen Fn. 27).
[1327] Siehe zum Software-VPN S. 53.
[1328] Vgl. bereits Fn. 9 und das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch“, S. 14, wo ausgeführt wird, dass ein Benutzer nach der erfolgreichen Anmeldung am directVPN mit anderen angemeldeten Computern Daten austauschen kann.
[1329] Siehe S. 307.
[1330] Siehe zum Online-Backup S. 74/ 82.
[1331] Siehe zu diesem Begriff S. 126.

einer selbständigen Datenablage auf dem Server des VPN-Auftraggebers erfolgt dies aus Sicht des Nutzers anwendungsdiensteunabhängig. Für ihn steht nicht der Inhalt der Daten im Vordergrund, sondern die Funktionsfähigkeit der Übertragung.
Für den VPN-Auftraggeber ist zwar möglicherweise der seitens des Nutzers übertragene Dateninhalt von erheblichem Interesse. Er bietet jedoch als Diensteanbieter keinen Inhalt oder keine Informationen an, die ein Nutzer als Nutzer eines Teledienstes gemäß § 2 Abs. 2 Nr. 1 TDG abrufen könnte.
So stellt der VPN-Auftraggeber lediglich eine technische Möglichkeit bereit, die den Empfang von Daten gemäß § 3 Nr. 23 TKG gewährleisten kann, so dass es sich um eine Telekommunikationsmöglichkeit und Telekommunikationsanlage handelt.[1332]

In diesem Sinne ist auch ein Software-VPN[1333] zu bewerten, sofern der mittels der VPN-Software ausgerüstete Rechner in der Firmenzentrale nicht ebenso Daten zum Abruf für die Nutzer bereithält, sondern allein als Kommunikationsplattform genutzt wird, um den Nutzern bei bestehender VPN-Verbindung die Möglichkeit zu bieten, Daten untereinander auszutauschen.[1334] Hier ist die Benutzerverwaltung installiert.[1335] Zur Erinnerung ist nochmals darauf hinzuweisen, dass bei einem Software-VPN ein Server in der Firmenzentrale die Benutzerverwaltung enthalten kann, so dass sich an diesem sämtliche Benutzer anmelden müssen, um miteinander kommunizieren zu können. Dieser Server ist insoweit also eine notwendige Kommunikationsschnittstelle für den Datenaustausch der einzelnen Nutzer, ohne aber selbst Inhalte bereit zu stellen.
Damit stellt der VPN-Auftraggeber bei dieser Variante ebenso einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG bereit. Inwieweit der VPN-Auftraggeber gemäß §§ 91 ff. TKG hierbei allerdings geschäftsmäßig handelt wird unter der datenschutzrechtlichen Prüfung erörtert.[1336]

[1332] Zum weiten Verständnis einer Telekommunikationsanlage gemäß § 3 Nr. 23 TKG siehe Krader, Das neue Telekommunikationsrecht in der Praxis, S. 117. Außerdem S. 114, insbesondere Fn. 492..
[1333] Siehe S. 53.
[1334] Siehe hierzu oben Fn. 1328 unter Verweis auf Fn. 9.
[1335] Siehe S. 53.
[1336] Siehe S. 345 ff.

Zum Zwecke der klaren Abgrenzung ist hier ergänzend anzumerken, dass im Hinblick auf das Verhältnis der Nutzer untereinander etwas anderes gilt.[1337] Sind diese in einem Software-VPN verbunden und können aufgrund der bestehenden VPN-Verbindung Daten miteinander austauschen, so ist der Nutzer, der die Daten einem anderen Nutzer bereitstellt, Teledienstanbieter gemäß § 2 Abs. 2 Nr. 1 TDG. Es stehen die Individualkommunikation, der Inhalt sowie der Datenaustausch im Vordergrund, wobei derjenige, der die Daten empfängt, Nutzer dieses Teledienstes ist.

cc. Kombinierter Telekommunikations- und Teledienst

Stellt der VPN-Auftraggeber seinen Nutzern sowohl die Möglichkeit des Datenabrufs als auch der Datenübertragung bereit (Kombination der beiden vorangegangenen Dienste), so ist der Server in der Firmenzentrale einerseits „Datenempfangsanlage" und der VPN-Auftraggeber damit Diensteanbieter gemäß § 3 Nr. 6 TKG. Andererseits hält er ebenso Daten für die Nutzer zum Abruf bereit, so dass der Inhaltsbezug im Vordergrund steht und für diesen Teil das Teledienstegesetz gemäß § 2 Abs. 1 TDG Anwendung findet.

Für diese Sichtweise sollte im Übrigen nicht die hardwaretechnische Einheit im Sinne eines einzigen Gerätes entscheidend sein, sondern es sollte die Frage gestellt werden, welche unterschiedlichen Funktionen bzw. Dienste der einzelne Server bietet. So kann unter Umständen ein einziges Gerät (bzw. was das Auge eines Betrachters von außen als einziges Gerät betrachtet), sowohl Daten zum Abruf bereithalten als auch für eigenständige Zwecke des Datentransportes gemäß § 3 Nr. 22 TKG zur Verfügung stehen.

Im datenschutzrechtlichen Prüfungsteil soll die Frage beantwortet werden, welche Konsequenzen mit einer solchen Kombination verbunden sind.[1338]

[1337] Siehe S. 310 ff.
[1338] Siehe S. 345 ff.

c. Management des Gateways

Das Systemmanagement des Gateways durch den VPN-Auftraggeber[1339] beinhaltet die Erbringung eines Telekommunikationsdienstes gemäß § 3 Nr. 24 TKG, da von dort die Weiterleitung von Daten in „sein“ Firmennetz erfolgt. Der Gateway stellt eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG dar,[1340] die vom VPN-Auftraggeber betrieben wird. Die gilt unabhängig davon, ob das Systemmanagement im Sinne eines Komplettmanagements oder eines Splitmanagements erfolgt. Wesentlich ist vielmehr, dass sich der Gateway im Machtbereich des Auftraggebers befindet.[1341]
Hiervon abzugrenzen ist jedoch die Frage, inwieweit der VPN-Auftraggeber gegenüber den Nutzern, die auf dieses Gateway zugreifen und deren Daten durch dieses Gateway in das Unternehmensnetz weitergeleitet werden, einen geschäftsmäßigen Telekommunikationsdienst im Sinne von §§ 91 ff. TKG erbringt. Dies ist innerhalb der datenschutzrechtlichen Prüfung zu bewerten.[1342]

3. Zusatzdienst E-Mail

Im Hinblick auf den E-Mail-Dienst wurde festgestellt, dass es sich um eine reine Übertragung handelt und dass damit die Anwendung des TKG in Betracht kommt.[1343]
Der VPN-Auftraggeber stellt seinen Mitarbeitern durch die Zurverfügungstellung von E-Mail-Accounts einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG bereit. Damit bleibt im datenschutzrechtlichen Prüfungsteil die Frage zu beantworten, inwieweit der VPN-Auftraggeber gemäß §§ 91 ff. TKG geschäftsmäßig handelt.[1344]
Ein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG und damit die Transportbezogenheit des Dienstes steht allerdings dann nicht mehr im Vordergrund, sofern der Nutzer des E-Mail-Services bzw. der

[1339] Vgl. S. 49.
[1340] Siehe oben S. 148. Siehe zur Funktionsherrschaft etwa Bothe/Heun/Lohmann, ArchivPT 1995, 5, 18/20; Manssen in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 3 TKG(1998), Band 1, Rn. 3.
[1341] Vgl. hierzu die obigen Ausführungen auf S. 149 ff.
[1342] Siehe S. 335 ff.
[1343] Siehe S. 157 ff.
[1344] Siehe S. 357 ff.

Kommunikationsmöglichkeit kein Mitarbeiter ist, dem der VPN-Auftraggeber einen E-Mail-Account bereitstellt, sondern ein Nutzer, der die E-Mail erhält (beispielsweise ein Kunde oder Geschäftspartner). [1345] In Bezug auf dieses Personenverhältnis steht zwar die Inhaltsbezogenheit im Vordergrund, so dass ein Teledienst in Betracht kommen müsste.[1346] Dies hätte zur Folge,, dass aus Sicht des Nutzers jeder, der einen E-Mail-Account unterhält und E-Mails versendet, ebenso Telediensteanbieter gemäß § 2 Abs. 1 Nr. 1 TDG, § 3 Nr. 1 TDG ist (und hätte damit im Übrigen nicht nur Aussagekraft für einen VPN-Auftraggeber, sondern für jeden Versender einer E-Mail). Über das Merkmal der Inhaltsbezogenheit hinaus ist jedoch die gesetzliche Regelung des § 3 Nr. 1 TDG zu berücksichtigen, die für das Vorliegen eines Teledienstes gleichermaßen ein „Bereithalten" fordert.[1347]

Der Versender einer E-Mail hält aber keine Teledienste bzw. den Inhalt der E-Mail bereit. Unter dem Merkmal des Bereithaltens ist das Vorhalten eines Dienstes in eigenem Speicher zu verstehen, womit ebenso vorausgesetzt ist, dass der Anbieter eigener Teledienste über die zur Speicherung notwendigen technischen Einrichtungen verfügen muss.[1348]

Diesbezüglich ergibt sich aus dem obigen Bildbeispiel jedoch,[1349] dass der Versender die Verfügungsmacht über die Inhalte verliert, sobald er diese versendet hat, da diese auf dem PoP3 Server des E-Mail-Diensteanbieters bzw. Providers zum Abruf (für den Empfänger) bereit gehalten werden. Bezüglich dieses Servers übt der Provider sowohl die Funktionsherrschaft[1350] aus, und der Versender einer E-Mail kann noch nicht einmal über einen Teilspeicherplatz nach Belieben verfügen.[1351]

[1345] Siehe zum Begriff des Nutzers S. 302 ff. sowie S. 83 ff., S. 279 ff., S. 294 ff.,

[1346] Siehe zum Teledienst oben S. 67/67 und Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 89; Schuster in: TKG- Kommentar, § 4 TKG Rn. 4c; Schmitz in: Hoeren/Sieber, Teil 16.4 Rn. 45; Beck-IuKDG-Tettenborn, § 2 TDG Rn. 42; Pankoke, Von der Presse- zur Providerhaftung, S. 27; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 106 ff. (der hier die E-Mail-Adresse unter den Voraussetzungen des TDDSG prüft); zur Individualkommunikation von E-Mail vgl. auch Schaar, Datenschutz im Internet, Rn. 12 sowie Hobert, Datenschutz und Datensicherheit im Internet, S. 38.

[1347] Zum Begriff des Bereithaltens siehe ebenso Fn. 560.

[1348] Waldenberger in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDG Rn. 23.

[1349] Siehe S. 63.

[1350] Zur Funktionsherrschaft im Sinne des Ausübens der rechtlichen und tatsächlichen Kontrolle siehe oben S. 149 ff.

[1351] Vgl. hierzu Waldenberger in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDG Rn. 23.

Damit ist der Versender einer E-Mail weder als Diensteanbieter gemäß § 3 Nr. 6 TKG noch als Anbieter eines Teledienstes gemäß §§ 2 Abs. 2 Nr. 1, 3 Nr. 1 TDG zu qualifizieren. Die folgende datenschutzrechtliche Prüfung bezieht sich daher auf die Frage, ob und welche datenschutzrechtlichen Pflichten den VPN-Auftraggeber gegenüber dem E-Mail-Kommunikationspartner aus dem BDSG treffen können (insbesondere ob gegebenenfalls E-Mail-Adresse, Datum und Uhrzeit sowie Inhalt der E-Mail gelöscht werden müssen). [1352]

Hieraus wird im Übrigen ersichtlich, dass ebenso wenig der Provider durch die Bereitstellung des POP3-Mailservers Teledienstanbieter gemäß § 2 Abs. 2 Nr. 1 TDG ist. Denn zum einen hält der Provider weder fremde Teledienste bereit, da gerade festgestellt worden ist, dass der Versender einer E-Mail kein Telediensteanbieter gemäß § 3 Nr. 1 TDG ist. Zum anderen erbringt der Provider ebenso wenig einen eigenen Teledienst gemäß § 2 Abs. 2 Nr. 1 TDG, da er selbst kein Angebot zur Individualkommunikation erbringt und keine eigenen Inhalte bereitstellt. Er stellt lediglich dem seinem Vertragspartner (VPN-Auftraggeber) eine technische Möglichkeit zur Verfügung, die dieser in Anspruch nehmen kann, um Daten zu empfangen. Damit handelt es sich aber um Telekommunikation gemäß § 3 Nr. 23 TKG.[1353]
Zu betonen ist, dass sich dieses Ergebnis lediglich durch eine Gesamtschau sämtlicher Personenverhältnisse ermitteln lässt. Daher wird auch an dieser Stelle die Erforderlichkeit, sämtliche möglichen Personenverhältnisse eines Online-Dienstes zu untersuchen, nochmals verdeutlicht.

[1352] Siehe S. 357 ff. An diese Stelle sei bereits darauf verwiesen, dass die Prüfung sich nur auf die geschäftliche Kommunikation bezieht, da innerhalb des privaten Bereiches datenschutzrechtliche Belange gemäß § 1 Abs. 2 Nr. 3 BDSG nicht zu berücksichtigen sind.
[1353] Bei privatem E-Mail-Verkehr findet Datenschutz keine Anwendung (§ 1 Abs. 2 Nr. 3 BDSG).

4. Zwischenergebnis

Die rechtliche Untersuchung in dem hier untersuchten Personenverhältnis „Auftraggeber/Nutzer“ führt zu dem Ergebnis, dass die Anwendbarkeit des Client-Server-Prinzip[1354] sowie des OSI-Schichtenmodells[1355] für die Einordnung eines Dienstes als Telekommunikationsdienst oder Teledienst nicht zielführend sind. Ob im konkreten Einzelfall ein Telekommunikationsdienst, ein Tele- oder Mediendienst oder ein Internet-Dienst in Betracht kommt, ist vielmehr aus der jeweiligen Nutzersicht und dem Verwendungszweck zu entscheiden, da ein Angebot oder ein Dienst unterschiedliche Zielrichtungen haben kann.[1356] Die eingesetzte Technik und die unterschiedlichen Protokolle (Tunneling-Protokolle, ftp) können insoweit unterschiedliche Funktionen bzw. Angebote bieten und Basis sowohl von Telediensten als auch von Telekommunikationsdiensten sein.

Daher ist nicht die Technik bzw. der Internet-Dienst[1357] als Telekommunikationsdienst oder Teledienst einzuordnen, sondern die „dahinter stehenden“ Angebote sind entsprechend der gesetzlichen Regelungen gemäß § 2 Abs. 1 TDG oder § 3 Nr. 24 TKG rechtlich zu bewerten.[1358] So ist ein ftp-Angebot nicht notwendigerweise ein Teledienst, sondern es werden in der Praxis mittels dieses Protokolls lediglich regelmäßig Teledienste angeboten.[1359] Es können aber ebenfalls Telekommunikationsdienste angeboten werden. Dies wurde in den obigen Ausführungen deutlich gemacht.

[1354] Siehe S. 43 ff./125 ff./305 ff.
[1355] Siehe S. 22 ff./308 ff.
[1356] Siehe hierzu auch Krader in: Königshofen, Das neue Telekommunikationsrecht in der Praxis, S. 121/123, die am Beispiel von ftp ebenfalls danach unterscheidet, ob es für den Nutzer vorrangig auf den Erhalt spezifischer Informationen ankommt oder es ihm vorrangig um die Übertragung geht.
[1357] Siehe zum Begriff des Internet-Dienstes S. 75 ff.
[1358] Vgl. hierzu auch S. 122 ff.
[1359] Vgl. auch Schuppert, CR 2000, 227, 230 zum Hosting und der dort eingesetzten ftp-Technik.

II. Datenschutz innerhalb der Dienste im VPN

Entsprechend dem in dieser Arbeit angewendeten Prüfungsschema werden nachfolgend die datenschutzrechtlichen Pflichten der Datenvermeidung, technischen Schutzmaßnahmen sowie Auskunfts- und Überwachungsmaßnahmen in dem Personenverhältnis „VPN-Auftraggeber/Nutzer“ innerhalb der einzelnen Dienste des Komplettpakets VPN untersucht.[1360]

1. Internetverbindung

Die Bereitstellung einer Internetverbindung stellt eine Teilleistung innerhalb eines VPN dar.[1361] Hier stellt sich im Besonderen die Frage nach der effektiven Datenvermeidung und Löschung von Daten, was im Folgenden untersucht wird. Die Frage nach der Sicherstellung von technischen Schutzmaßnahmen oder Auskunfts- und Überwachungspflichten werfen bei dem Dienst „Bereitstellung einer Internetverbindung bzw. Internetzugangs“ hingegen keine besonderen Probleme auf.[1362] Daher werden diese datenschutzrechtlichen Pflichten bei den weiteren Diensten des Komplettpakets VPN (VPN-Kommunikation und Zusatzdienst E-Mail) näher behandelt.[1363]

a. Datenvermeidung nach BDSG

Im Rahmen der datenschutzrechtlichen Pflichten eines VPN ist in dem hier untersuchten Personenverhältnis zwischen den Möglichkeiten des zwangsweisen und freiwilligen Tunneling zu unterscheiden.

[1360] Vgl. S. 106 ff., 162 ff., 280 ff.
[1361] Vgl. S. 120 ff.
[1362] Vgl. zu dem Prüfungsschema in dieser Arbeit S. 106 ff.
[1363] Vgl. S. 345 ff., S. 365 ff.

aa. Zwangsweises Tunneling

Im Rahmen eines VPN kann die Internetnutzung zu ausschließlich beruflichen Zwecken durch zwangsweises Tunneling[1364] ermöglicht werden. Denn damit wäre sichergestellt, dass bei Einwahl in das Internet ein Verbindungsaufbau stets nur zu den jeweiligen Standorten erfolgt. Dies setzt außerdem voraus, dass der VPN-Auftraggeber den Zugriff ferner so gestaltet, dass lediglich bestimmte, unternehmensrelevante Dateien ausgetauscht werden können und ein Zugriff nur auf unternehmensrelevante Ordner erfolgt. Eine Möglichkeit wäre hier beispielsweise, unterschiedliche Laufwerke („öffentlich" und „privat") anzulegen. Durch die technische Maßnahme des zwangsweisen Tunneling kann der Arbeitgeber daher von vorneherein Einfluss auf die betriebliche und private Kommunikation des Nutzers bzw. Arbeitnehmers nehmen. Dies gilt allerdings nur, sofern dem Arbeitnehmer kein weiterer Internetzugang zur Verfügung gestellt wird, mit dem eine private Internetnutzung möglich wäre (freiwilliges Tunneling).[1365] Ist der Zugriff auf private Dateien jedoch nicht ausgeschlossen, muss darüber hinaus seitens des VPN-Auftraggebers (bzw. Arbeitgebers) gegenüber den Nutzern eine separate Anweisung dahingehend erfolgen, das VPN ausschließlich zu beruflichen Zwecken zu nutzen, und die private Nutzung zu verbieten.

Dies führt zu der Besonderheit, dass sich der Datenschutz nach dem BDSG richtet,[1366] obwohl bei der Bereitstellung des Internetzugangs grundsätzlich ein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG vorliegt.[1367]
Dies ist damit zu begründen, dass die Regelungen der §§ 91 ff. TKG geschäftsmäßiges Handeln voraussetzen, also ein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG an Dritte erbracht werden muss (vgl. auch § 3 Nr. 10 TKG). Die Eigenschaft als Dritter muss jedoch dann ausscheiden, sofern allein

[1364] Siehe zur Definition des zwangsweisen Tunneling S. 57 ff. Diese Technik wird im Übrigen allein bei Bereitstellung von Internet-Zugängen an Unternehmensstandorten in Betracht kommen, da bei Telearbeitsplätzen im häuslichen Bereich eines Arbeitnehmers der Internetzugang regelmäßig auch für private Zwecke genutzt wird.
[1365] Siehe hierzu nachfolgend auf S. 331 ff.
[1366] Bei ausschließlich beruflicher Nutzung des Internetzugangs durch die Arbeitnehmer wird vertreten, dass das BDSG zu beachten ist, etwa §§ 9, 28, 33 ff. BDSG. Siehe zur Anwendbarkeit des BDSG im Rahmen von Dienstgesprächen Mengel, BB 2004, 1445, 1447. Siehe zur Anwendbarkeit des BDSG für das „Innenverhältnis" Arbeitgeber-Arbeitnehmer im Rahmen von Telearbeit Wedde, NJW 1999, 527, 533.
[1367] Siehe S. 304.

die dienstliche Nutzung erlaubt ist.[1368] Denn in diesem Falle bilden Mitarbeiter und Arbeitgeber insoweit eine Kommunikationseinheit.[1369] Der Mitarbeiter bzw. Nutzer ist in diesen Fällen kein Dritter im Sinne von § 3 Nr. 10 TKG.[1370] Als Dritter ist in diesem Zusammenhang jede natürliche oder juristische Person außerhalb der verantwortlichen Stelle anzusehen (§ 3 Abs. 8 BDSG).[1371]

Grundsätzlich muss im Sinne der obigen Auslegung zwar beachtet werden, dass die Regelungen der §§ 91 ff. TKG vorrangig bei Telekommunikationsdiensten zur Anwendung kommen.[1372] Aufgrund dessen, dass der VPN-Auftraggeber hier jedoch keinen Telekommunikationsdienst für Dritte anbietet, finden §§ 91 ff. TKG generell keine Anwendbarkeit, so dass mangels Exklusivitätsverhältnis auf die Regelungen des BDSG zurückgegriffen werden darf. Dies zeigt sich insbesondere daran, dass in § 3 Nr. 24 TKG nunmehr kein gewerbliches oder geschäftsmäßiges Handeln mehr vorausgesetzt ist, so dass es ebenso Telekommunikationsdienste „ohne geschäftsmäßiges“ Handeln gibt. Zu berücksichtigen ist aber, dass Anbieter geschäftsmäßig handeln müssen, um den datenschutzrechtlichen Regelungen der §§ 91 ff. TKG zu unterfallen. [1373]

Gleichwohl kann eine umfassende Speicherung der Nutzungsdaten nicht in Betracht kommen. Die Anwendbarkeit von § 28 Abs. 1 Nr. 1 BDSG und eine zulässige Speicherung sämtlicher[1374] Nutzungsaktivitäten der Mitarbeiter im

[1368] Vgl. insbesondere Post-Ortmann, RDV 1999, 102, 103, die anmerkt, dass der Gesetzgeber die Nutzung von betrieblichen TK-Anlagen ausschließlich zu betrieblichen Zwecken seitens der Arbeitnehmer nicht mit den Vorschriften der §§ 85 ff. TKG a.F. gleichsetzen wollte. Siehe zum Protokollierungsrecht etwa Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 79; Gola/Schomerus, BDSG, § 28 BDSG Rn. 20; Gola/Klug, Grundzüge des Datenschutzrechts, S. 198; Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 40 ff., S. 75; Gola, MMR 1999, 322, 325.

[1369] Vgl. Post-Ortmann, RDV 1999, 102, 103, die bei privater Nutzung den Beschäftigten als Dritten sieht, da er die Telekommunikationseinrichtung außerhalb des Arbeitsbereiches und somit zu eigenen Zwecken nutzt. Im Umkehrschluss bedeutet dies aber auch, dass der Beschäftigte bei der Nutzung innerhalb des Arbeitsbereiches Zwecke des Arbeitgebers verfolgt und damit insoweit eine Identität vorliegt.

[1370] Vgl. Gola, MMR 1999, 322, 325, der bei einem Verbot der Privatnutzung die Eigenschaft als Dritter verneint; Gola/Klug, Grundzüge des Datenschutzrechts, S. 198; Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 75.

[1371] Zum Begriff des Dritten vgl. auch Gola/Schomerus, BDSG, § 3 BDSG Rn. 52.

[1372] Siehe auch § 1 Abs. 3 BDSG, § 1 Abs. 2 TDSV sowie die Ausführungen auf S. 92.

[1373] Gemäß § 3 Nr. 18 TKG a.F. umfasste der Begriff Telekommunikationsdienstleistung noch ein gewerbliches Angebot.

[1374] Sofern allein die dienstliche Nutzung erlaubt ist, wird regelmäßig die Auffassung vertreten, dass die Nutzung des Internet und der E-Mail-Verkehr umfassend protokolliert werden darf.

Internet wird zwar mit der Begründung bejaht, dass der Arbeitgeber die Überwachung der Nutzungsgewohnheiten seiner Arbeitnehmer feststellen können muss, insbesondere ob sich diese vertragstreu verhalten oder ihm gar durch ihre Internetnutzung einen Teil der geschuldeten Arbeitsleistung vorenthalten.[1375] Diese Auffassung geht jedoch fehl, denn zum einen ist im Rahmen von § 28 Abs. 1 Nr. 1 BDSG erforderlich, dass die Daten zur Erfüllung der Pflichten oder zur Wahrnehmung der Rechte aus dem Vertrag gespeichert werden müssen.[1376] Von einer solchen unerlässlichen Notwendigkeit kann jedoch im Rahmen der Speicherung der Internetnutzungsdaten des Arbeitnehmers hinsichtlich einer Leistungskontrolle nicht gesprochen werden. Ein solches Recht kann sich lediglich auf die Protokollierung zur Datenschutzkontrolle, zur Datensicherung und zur Sicherstellung des ordnungsgemäßen Betriebs der Datenverarbeitungsanlage beziehen.[1377] Denn diesbezüglich erfordern die arbeitsvertraglichen Beziehungen eine Speicherung dieser Nutzungsdaten, da dies die Voraussetzung dafür ist, den Betrieb aufrechterhalten zu können.[1378] Die Datenverarbeitung dient hier also als Mittel zum Zweck.[1379]

Insoweit kann daher als Zulässigkeitsregelung für die Protokollierung von Nutzungsaktivitäten der Mitarbeiter hinsichtlich einer Verhaltens- und Leistungskontrolle nicht § 28 Abs. 1 Nr. 1 BDSG sondern nur § 28 Abs. 1 Nr. 2 BDSG in Betracht kommen, mit der Konsequenz, dass eine Interessenabwägung stattfindet.[1380] Die Leistungskontrolle stellt keine Notwendigkeit dar, die erfolgen muss, um den Betrieb aufrechtzuerhalten, wenn

---

Siehe etwa Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 79; Gola/Schomerus, BDSG, § 28 BDSG Rn. 20; Gola/Klug, Grundzüge des Datenschutzrechts, S. 198; Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 40 ff., S. 75; Gola, MMR 1999, 322, 325; Hilber/Frik, RdA 2002, 89, 92 ff. (insbesondere S. 94).

[1375] Hanau/Hoeren/Andres, Private Internet-Nutzung durch Arbeitnehmer, S. 52. Siehe zu den vielfältigen technischen Möglichkeiten zur Kontrolle betrieblicher Netzwerke Hilber/Frik, RdA 2002, 89, 90; Hornung, MMR 2004, 3, 7; Büllesbach in: Roßnagel, Handbuch Datenschutzrecht, 6.1 Rn. 81.

[1376] Gola/Schomerus, BDSG, § 28 BDSG Rn. 13, die die Erforderlichkeit der Speicherung im Sinne eines „Müssen“ als herrschend bezeichnen. Vgl. zur Erforderlichkeit außerdem Däubler, NZA 2001, 874, 876.

[1377] Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 79.

[1378] Auch bei öffentlichen Stellen ist ein direkter Rückgriff auf § 14 Abs. 4 BDSG, der wegen § 12 Abs. 4 BDSG ohnehin ausgeschlossen ist, daher nicht notwendig, da hier die Zweckbestimmung des Arbeitsvertrages die ausreichende Legitimationsgrundlage bildet. Für die unmittelbare Anwendung von § 14 Abs. 4 BDSG siehe Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 79.

[1379] Gola/Schomerus, BDSG, § 28 BDSG Rn. 4.

[1380] Zu den Voraussetzungen des § 28 Abs. 1 Nr. 2 BDSG im Einzelnen siehe insbesondere die folgenden Ausführungen auf S. 393 ff.

es der Betroffene gar nicht anstrebt bzw. will. Dies liefe daraus hinaus, den Betroffenen vor sich selbst zu schützen. Denn hier geht es vorrangig nicht um die Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen bzw. Arbeitnehmer, sondern um die Wahrung der Interessen des VPN-Auftraggebers bzw. Arbeitgebers.

Daher darf der VPN-Auftraggeber an dem Standort, an welchem der Internetzugang bereitgestellt wird, Datum, Uhrzeit, Datenmenge, Dauer der Internetnutzung sowie Dateninhalte zwar grundsätzlich protokollieren.[1381] Diese Protokollierung darf aber im Rahmen einer Nutzung zu ausschließlich beruflichen Zwecken nur erfolgen, sofern dies für den ordnungsgemäßen Betrieb unbedingt erforderlich ist, da ein nicht ordnungsgemäßer Betrieb ebenso Auswirkung auf das Arbeitsverhältnis hat. Die Protokollierung darf dabei nicht zur Leistungskontrolle erfolgen, es sei denn es sprechen berechtigte Interesse[1382] für eine solche Datenverarbeitung.[1383] Da aber § 28 Abs. 1 Nr. 2 BDSG als Anknüpfungspunkt einer nur ausnahmsweise zulässigen Verarbeitung angesehen wird,[1384] sprechen die schutzwürdigen Interessen der Arbeitnehmer regelmäßig gegen eine solche Aufzeichnung, wenn keine konkreten Anzeichen für eine Störung des Arbeitsverhältnisses oder des Betriebs, dessen ordnungsgemäßer Ablauf Voraussetzung für die Erbringung der Arbeitsleistung ist, vorliegen. Eine Leistungskontrolle kommt allenfalls im Hinblick auf die verbotene Privatnutzung des Internet oder bei konkretem

---

[1381] Vgl. auch Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 75. Siehe auch Büllesbach in: Roßnagel, Handbuch Datenschutzrecht, 6.1 Rn. 82, der die Anwendung der datenschutzrechtlichen Regelungen wegen § 1 Abs. 1 TDDSG, § 16 Abs. 1 MDStV ausschließen möchte. Oben wurde jedoch ausführlich dargestellt, dass der Arbeitgeber, der die Internetnutzung für seine Arbeitnehmer bereitstellt, kein Diensteanbieter im Sinne von § 2 Abs. 2 Nr. 3 TDG darstellt, so dass von vorneherein die Anwendbarkeit des TDDSG ausscheiden muss.

[1382] Auernhammer, BDSG, § 28 BDSG Rn. 18, der darauf verweist, dass es sich hierbei um ein tatsächliches Interesse wirtschaftlicher oder ideeller Natur handeln kann.

[1383] Vgl. oben S. 322 sowie Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 79. Vgl. außerdem Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 78, der auf das Erfordernis der schriftlichen Einwilligung hinweist und darauf, dass die Erfassung von Kontrolldaten nicht der Zweckbestimmung des Arbeitsvertrages gemäß § 28 Abs. 1 Nr. 1 BDSG entspricht, wobei auch ebenso wenig das Interesse des Arbeitgebers an der Speicherung der Kontrolldaten den schutzwürdigen Interessen der Betroffenen nach § 28 Abs. 1 Nr. 2 BDSG überwiegt. Siehe auch Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 108 zur restriktiven Verarbeitung bei Internetanschlüssen und auf E-Mail-Servern gespeicherter Daten, die nicht durch die Organisationsbefugnis und das Aufsichtsrecht der Arbeitgeber gedeckt ist.

[1384] Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 91.

Verdacht strafbarer Handlungen in Betracht, wobei die Beteiligungsrechte des Betriebsrats zu beachten sind.[1385]

Der VPN-Auftraggeber hat dementsprechend erstellte Protokolle gemäß § 35 Abs. 2 Nr. 3 BDSG zu löschen, wenn er sie für seine Zwecke (z.B. Sicherstellung des ordnungsgemäßen Betriebs der Datenverarbeitungsanlage) nicht mehr benötigt.[1386]
Daher muss jeder VPN-Auftraggeber prüfen, ob und vor allem für welchen Zeitraum er Protokolle notwendigerweise aufbewahren muss, so dass er zur Prüfung in regelmäßigen Abständen, z.B. wöchentlich, monatlich oder quartalsweise verpflichtet sein muss, und zwar dahingehend, ob eine weiterhin andauernde Speicherung für die Aufrechterhaltung des ordnungsgemäßen Betriebs notwendig ist.[1387] Denn zu berücksichtigen ist, dass zur zukünftigen Gewährleistung des ordnungsgemäßen Betriebs ebenso die zukünftig erstellten Protokolle ausreichen können.

Die Zeiträume für die Aufbewahrung der Protokolle muss der jeweilige Betrieb in pflichtgemäßem Ermessen auf seine speziellen Erfordernisse abstimmen. Pauschal wird beispielsweise für Mail-Server vertreten, dass ein Zeitrahmen von zwei Wochen ausreichen sollte, da nach dieser Zeitspanne Fehler ohnehin nicht mehr korrigiert werden könnten.[1388] Es ist vertretbar, diese Zeitspanne ebenso bei anderen Systemen zugrunde zu legen, da Fehler stets und systemunabhängig in einem möglichst kurzen Zeitraum gefunden und behoben werden müssen. Im Einzelfall muss allerdings die nachvollziehbare Begründung möglich bleiben, aus welchem Grunde die Fehlersuche sowie Fehlerbehebung und die damit verbundene Datenspeicherung (ausnahmsweise) einen längeren Zeitraum benötigt.[1389] .

[1385] Siehe zu den Beteiligungsrechten des Betriebsrats S. 328 ff. sowie zur Verhaltens- und Leistungskontrolle in diesem Zusammenhang ebenso die Ausführungen zur E-Mail-Nutzung S. 358 ff. Vgl. außerdem Däubler, K&R 2000, 323, 327.
[1386] Vgl. aber auch Hilber/Frik, RdA 2002, 89, 94, die eine umfassende Protokollierung von Arbeitnehmerdaten erlauben, ohne Rückgriff auf das BDSG zu nehmen.
[1387] Siehe Bizer in: Simitis, BDSG-Kommentar, § 3a BDSG Rn. 54 zu den technisch unterstützten Löschungs- oder zeitlich wiederkehrenden Prüfroutinen zur Erfüllung des Systemdatenschutzes.
[1388] Vgl. hierzu Gerling, DuD 2005, 338, 339. Siehe auch S. 180.
[1389] Siehe zur grundsätzlich restriktiven Auslegung des Rechts auf Protokollierung, Bizer, DuD 2006, S. 270, 273. Siehe zu den Vorgaben einer Speicherdauer und einer am Einzelfall

Festzustellen ist insgesamt, dass bei der Nutzung von Kommunikationseinrichtungen der Arbeitgeber das verfassungsrechtlich garantierte Persönlichkeitsrecht des Arbeitnehmers aus Artikel 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, das Fernmeldegeheimnis gemäß Artikel 10 Abs. 1 GG sowie die datenschutzrechtlichen Vorgaben beachten muss.[1390] Die Überwachung von Arbeitnehmern durch den Einsatz von Datenverarbeitungsanlagen stellt eine Datenerhebung oder –verarbeitung dar, auch wenn die Datenverarbeitung nicht primär diesem Zweck dient, so dass der Grundsatz der Verhältnismäßigkeit gewahrt werden muss.[1391]

Das Bundesverfassungsgericht hat in diesem Zusammenhang das Recht des Einzelnen hervorgehoben, seine Kommunikationspartner selbst zu bestimmen und unbeobachtet mit ihnen in Verbindung zu treten und diesen Grundsatz ausdrücklich auch auf die Beziehungen zwischen Arbeitgeber und Arbeitnehmer erstreckt.[1392] Soll eine Ausnahme von diesem Grundsatz gemacht werden, so müssen berechtigte Interessen des Arbeitgebers vorliegen. Solche berechtigten Interessen können wie oben bereits angesprochen die Fehlerkontrolle oder die Systemsicherheit darstellen. Zu berücksichtigen ist aber, dass der Arbeitgeber nicht „durch eine solche Hintertür" das Verhalten seiner Mitarbeiter kontrollieren darf.

In einem anderen Zusammenhang hat jedoch der 2. Senat des BAG in seiner Entscheidung vom 27.03.2003 eine heimliche Kontrolle von Arbeitnehmerverhalten durch Videoaufzeichnung für zulässig erachtet, [1393] wohingegen der 1. Senat des BAG in seinen Beschlüssen vom 29.06.2004 und 14.12.2004 festgestellt hat, dass bereits die offene Verwendung von

orientierten Betrachtungsweise auch Schoen, DuD 2005, S. 84, 86 (der sich in seinen Ausführungen allerdings auf die gesetzliche Grundlage des TDDSG bezieht).

[1390] Vgl. auch Däubler in: Ahrens/Donner/Simon, Arbeit-Umwelt, 2001, S. 1, 6; Nägele, ArbRB 2002, 55, 56. Mengel, BB 2004, 1445, 1448; Mengel, BB 2004, 2014, 2015. Zu den Persönlichkeitsrechten eines Arbeitnehmers wird im Rahmen der nachfolgenden Ausführungen im Übrigen nochmals differenzierter Stellung genommen. Diese befassen sich im Besonderen sowohl mit „privater Internetnutzung" als auch mit „dienstlicher und privater E-Mail-Nutzung" (siehe insbesondere auch S. 360).

[1391] Fleck, BB 2003, 306, 308.

[1392] BVerfG NJW 1992, 815, 815. Vgl. auch Tinnefeld/Viethen, NZA 2000, 977, 979 dort Fn. 34 mit Verweis auf die Entscheidung des BVerfG. Menzel, NJW 1989, 2041, 2042. Siehe zur mittelbaren Drittwirkung der Grundrechte um Arbeitsverhältnis auch Oetker, RdA 2004, 8, 11, der ausführt, dass diese Grundrechtsbindung die zivilrechtlichen Generalklauseln (§§ 138, 242 BGB) beeinflusst. In diesem Sinne auch Jarass, NJW 1989, 857, 862.

[1393] Siehe BAG (2. Senat) AuR 2005, 453 ff. zur Frage der Zulässigkeit der Videoüberwachung von Arbeitnehmern.

Videoüberwachungsanlagen nur ausnahmsweise erlaubt ist.[1394]. In seiner Begründung stellt das 2. Senat des BAG fest, dass die heimliche Videoüberwachung zwar einen Eingriff in das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht des Arbeitnehmers darstelle. Dies führe aber nicht zu einem Beweisverwertungsverbot, wenn der konkrete Verdacht einer strafbaren Handlung oder einer schwerwiegenden Verfehlung zu Lasten des Arbeitgebers bestehe und die verdeckte Videoaufzeichnung praktisch das einzig verbleibende Mittel darstelle und insgesamt nicht unverhältnismäßig ist.[1395] Diese Entscheidung ist zu Recht kritisiert worden. [1396] In einer Stellungnahme zu diesen Entscheidungen wird darauf verwiesen, dass das BAG im Hinblick auf das „einzig verbleibende Mittel“ der notwendigen Auseinandersetzung mit der Frage aus dem Weg gegangen ist, ob der Arbeitgeber nicht ebenso auf die Alternative der Einschaltung der Strafverfolgungsbehörden hätte zurückgreifen können. Zum anderen bezieht sich die Kritik darauf, dass keine Beschäftigung mit der Frage erfolgt ist, ob in der konkreten Ausgestaltung der Arbeitsabläufe ebenso ein massives Organisationsversagen des Arbeitgebers gesehen werden könnte.[1397]Dieser Auffassung ist zuzustimmen, da in diesem Zusammenhang zu berücksichtigen ist, dass die grundrechtlich (ebenso) geschützte unternehmerische Betätigungsfreiheit des Arbeitgebers (die in diesem Fall aus Art. 14 GG hergeleitet werden kann), [1398] bereits aus diesen Gründen nicht

[1394] BAG (1. Senat) AuR 2005, 453, 454 sowie AuR 2005, 453, 456 zur Frage der Zulässigkeit der Videoüberwachung von Arbeitnehmern. Siehe auch Wedde, AuR 2005, 453, 457.
[1395] Siehe BAG (2. Senat) AuR 2005, 453 ff. zur Frage der Zulässigkeit der Videoüberwachung von Arbeitnehmern.
[1396] Siehe die ablehnende Stellungnahme von Wedde, AuR 2005, 453, 457 ff., insbesondere unter Verweis auf die mangelnde Berücksichtigung der Vorgaben der EU-Datenschutzrichtlinie 95/56/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (siehe Wedde aa0 S. 458).
[1397] Siehe Wedde aaO.
[1398] Siehe auch die Verweise zur wirtschaftlichen Betätigungsfreiheit auf S. 422 und in dort Fn. 1843. Art. 14 Abs. 1 GG schützt das Erworbene, das Ergebnis einer Betätigung, Art. 12 Abs. 1 GG schützt dagegen den Erwerb, die Betätigung selbst (Vgl. BVerfGE 30, 292, 334/335; Dieterich in: Erfurter Kommentar, Art. 12 GG Rn. 16). Bei der Abgrenzung zwischen Art. 12 Abs. 1 GG und Art. 14 Abs. 1 GG gilt die Meistbetroffenheitsregel (Dieterich in: Erfurter Kommentar, Art. 12 GG Rn. 16 und Art. 14 GG Rn. 9), da Art. 12 GG durch Art. 14 GG grundsätzlich nicht verdrängt wird (BVerfGE 50, 291, 361. Teilweise lässt das Bundesverfassungsgericht die Konkurrenz zwischen Art. 12 GG und Art. 14 GG auch dahinstehen, sofern bereits der Schutzbereich eines Grundrechts bejaht wird (vgl. BVerfGE 22, 380, 386)). Entscheidend ist daher für die Abgrenzung zwischen Berufsfreiheit und Eigentumsgewährleistung, ob eher die Freiheit der individuellen Erwerbs- und Leistungstätigkeit oder die Innehabung und Verwendung vorhandener Vermögensgüter durch einen Akt öffentlicher Gewalt betroffen ist (Wieland in: Dreier, GG-Kommentar, Art. 14 GG Rn. 183).

überwiegen kann, da die heimliche Überwachung nicht das einzige verbleibende Mittel darstellt.
Insgesamt ist daher ebenso wenig unter diesen Gesichtspunkten eine andere Bewertung von Arbeitnehmerkontrollen gerechtfertigt.[1399]

bb. Nutzungsdetails

Regelmäßig ist auch bei einem zentralen firmenseitigen Zugang ins Internet unternehmensintern nachvollziehbar, welcher Nutzer zu welchem Zeitpunkt und für welchen Zeitraum im Internet gesurft hat.[1400] Denkbar wäre darüber hinaus die Aufzeichnung der angewählten IP-Adressen oder Domain-Namen (bzw. Websites). [1401]
Aus den obigen Ausführungen ergibt sich, dass der Arbeitgeber beim zwangsweisen Tunneling berechtigt ist, diese Nutzungsdetails ohne besondere Einwilligung[1402] der Arbeitnehmer bzw. Nutzer zu protokollieren. Allerdings darf er dies nicht, um damit die Leistung seiner Mitarbeiter zu kontrollieren.[1403]

Problematisch ist bei der Erstellung einer Protokolldatei zum Zwecke der Gewährleistung der Systemsicherheit, dass bei ihrer Durchsicht ebenso auffallen kann und wird, wie oft, zu welchem Zeitpunkt und für welchen Zeitraum ein bestimmter Mitarbeiter Unternehmensstandorte angewählt hat und gegebenenfalls in welche Dateien er Einsicht genommen hat.

[1399] Siehe in diesem Zusammenhang insbesondere auch Wedde, AuR 2005, 453, 459 mit dem Hinweis auf die bislang fehlende Verabschiedung eines Gesetzes zum Arbeitnehmerdatenschutz.
[1400] Dies lässt sich anhand der so genannten MAC-Adresse (MAC bedeutet Medium Access Control) feststellen; siehe hierzu ausführlich Davis, IPSec, S. 18 ff., der darauf verweist (S. 18), dass die MAC-Adresse auch Hardware-Adresse genannt wird. Siehe außerdem Dornseif/Schumann/Klein, DuD 2002, 226, 227. Jede Netzwerkkarte in den Computern verfügt über eine weltweit eindeutige MAC-Adresse. Damit kann auch innerhalb eines Unternehmens, welches über einen zentralen Internetzugang verfügt, an dieser Zentrale (Server) leicht der jeweilige Computer und damit auch dessen Nutzer zurückverfolgt werden. Vgl. allerdings auch Dornseif/Schumann/Klein, DuD 2002, 226, 227 mit dem Hinweis, dass der Benutzer eines Computers die MAC-Adresse leicht ändern kann.
[1401] Siehe hierzu auch die Ausführungen auf S. 183 ff. und S. 280 ff. zu der Frage, inwieweit die Speicherung der IP-Adressen und Domain-Namen zulässig ist, insbesondere in Verbindung mit einem Einzelverbindungsnachweis. Vgl. auch Mengel, BB 2004, 1445, 1449 zur Zulässigkeit der Speicherung der Zielrufnummer bei Dienstgesprächen.
[1402] Vgl. § 4a BDSG.
[1403] Siehe Haft/Eisele, JuS 2001, 112, 115 zur technischen Möglichkeit der Nachrichtenaufzeichnung.

Zu berücksichtigen ist außerdem, dass für den Arbeitgeber in einem Kündigungsschutzprozess ein Beweisverwertungsverbot, wenn er aufgrund einer unzulässigen Kontrollmaßnahme ein pflichtwidriges Telekommunikationsverhalten eines Arbeitnehmers feststellt.[1404]
Insgesamt muss sichergestellt sein, dass der Arbeitgeber seine Mitarbeiter nicht „durch die Hintertür" kontrolliert. Das Ziel der Aufrechterhaltung des Betriebes kann sich allein auf technische Begebenheiten beziehen, insbesondere darauf, die Stabilität der Systeme durch permanente Fehlerkontrolle sicherzustellen. Dabei darf nicht in die Prüfung mit einfließen, ob der Betriebsablauf etwa dadurch gestört sein könnte, dass ein Mitarbeiter mehr Zeit im Internet zu privaten Zwecken verbringt als sich um seine eigentliche, durch den Arbeitsvertrag bestimmte Aufgabe zu kümmern. Denn dies stellt eine Kontrolle des Leistungsverhaltens dar, die der Einwilligung des Arbeitnehmers bedarf, und die aufgrund der Regelung des § 75 Abs. 2 BetrVG (Betriebsverfassungsgesetz) im Übrigen nicht wirksam durch eine Betriebsvereinbarung ersetzt werden könnte.[1405] Auch eine Betriebsvereinbarung kann daher nur insoweit zulässig sein, wie sie nicht den Grundsatz der in Art. 1 und 2 GG geforderten Schutz der Persönlichkeitsrechte verletzt.[1406]

Aufgrund der möglichen Kontrolle des Leistungsverhaltens stellt aber zumindest die Beteiligung eines bestehenden Betriebsrates eine wichtige Schutzfunktion bei der Protokollierung der Internetnutzungsdetails von Arbeitnehmern dar. Es ist daher zu berücksichtigen, dass die Einführung von betrieblichen

---

[1404] Siehe etwa LAG Niedersachsen, MMR 2002, 766, 767; Beckschulze, DB 2003, 2777, 2782; Mengel, BB 2004, 1445, 1451. Siehe ebenso Nägele/Meyer, K&R 2004, 312, 316.

[1405] Siehe zu den Grenzen der Betriebsvereinbarung Wedde, DuD 2004, 169, 174. Siehe zum Recht auf informationelle Selbstbestimmung im Arbeitsverhältnis außerdem Wedde, Telearbeit, S. 136 ff. Siehe aber beispielsweise zur Zulässigkeit von Taschen-, Fahrzeug- oder Personenkontrollen unter Berücksichtigung der persönlichen Freiheit und Würde des Arbeitnehmers Berg in: Däubler/Kittner/Klebe, BetrVG, § 75 BetrVG Rn. 37. Ergänzend sei angemerkt, dass es in den Fällen keiner Einwilligung des Arbeitnehmers bedarf, in denen sich das Mitbestimmungsrecht des Betriebsrats gerade auf den Schutz des Arbeitnehmers bezieht. Dies gilt insbesondere gemäß § 87 Nr. 2 BetrVG im Hinblick auf die werktägliche Höchstarbeitszeit sowie Ruhepausen (siehe auch Klebe in: Däubler/Kittner/Klebe, BetrVG, § 87 Nr. 2 BetrVG Rn. 68 ff. Siehe zur Zulässigkeit der Speicherung von Soll- und Ist-Arbeitszeit gemäß § 28 Abs. 1 Nr. 1 BDSG Däubler, Gläserne Belegschaften?, Rn. 260.

[1406] Vgl. Weißnicht, MMR 2004, 448, 453; Wedde, DuD 169, 173/174. Siehe zum Schutzauftrag des § 75 Abs. 2 BetrVG Bantle in: Kittner/Zwanziger, Arbeitsrecht, § 113 Rn. 39 ff, insbesondere auch die Ausführungen in Rn. 46 , in denen auf die Auflösung des Betriebsrates bei erheblichem Verstoß gegen § 75 BetrVG verwiesen wird.

Informations- und Kommunikationseinrichtungen, die diese Protokollierung ermöglichen, der Mitbestimmung des Betriebsrates unterliegen. Entsprechende Mitbestimmungsrechte sind in § 87 Abs. 1 Nr. 1 und Nr. 6 Betriebsverfassungsgesetz (BetrVG)geregelt.[1407]

§ 87 Abs. 1 Nr. 1 BetrVG bezieht sich auf Fragen der Ordnung des Betriebs sowie des Verhaltens der Arbeitnehmer im Betrieb[1408] und erfasst Verhaltensregeln der Arbeitnehmer, durch die ein geordnetes Zusammenleben und Zusammenwirken im Betrieb und damit ein reibungsloses Funktionieren des Betriebes gewährleistet werden soll.[1409] Verhaltensregeln für Mitarbeiter werden etwa dann aufgestellt, wenn festgelegt wird, in welchem Zeitrahmen ein Mitarbeiter höchstens Zeit im Internet verbringen darf. Im Hinblick auf ein VPN wäre § 87 Nr. 1 BetrVG betroffen, wenn in einem Unternehmen die VPN-Nutzung für sämtliche Mitarbeiter verbindlich eingeführt werden soll.

Allein die Verwendung bzw. Einführung von betrieblichen Informations- und Kommunikationseinrichtungen stellt jedoch keine Maßnahme dar, die das Ordnungsverhalten im Betrieb regelt.

Bezüglich der Einführung von *technischen* Einrichtungen, die eine Überwachung der Mitarbeiter ermöglichen, ist daher der Tatbestand des § 87 Nr. 6 BetrVG viel wichtiger.[1410] § 87 Abs. 1 Nr. 6 BetrVG geht als lex specialis § 87 Abs. 1 Nr. 1 BetrVG vor, soweit eine Verhaltens- oder Leistungskontrolle

[1407] Nägele, ArbRB 2002, 55, 56; Däubler in: Ahrens/Donner/Simon, Arbeit-Umwelt, 2001, S. 1, 6; Altenburg, v. Reinersdorff, Leister, MMR 2005, 222, 223; BAG AP Nr. 2 zu § 87 BetrVG 1972 „Überwachung“; BAG AP Nr. 7 zu § 87 BetrVG „Überwachung“; wo darauf verwiesen wird, dass durch eine technisierte Ermittlung von Verhaltens- und Leistungsdaten eine ungleich größere Anzahl von Informationen erhoben werden kann. Vgl. aber andererseits LAG Hamm MMR 2006, 700 ff. zum fehlenden Mitbestimmungsrecht des Betriebsrats beim betrieblichen Verbot der Privatnutzung des Internet- und E-Mail-Verkehrs.

[1408] Klebe in: Däubler/Kittner/Klebe, BetrVG, § 87 BetrVG Rn. 42. Siehe hierzu auch Nägele, ArbRB 2002, 55, 59. Kania in: Erfurter Kommentar, § 87 BetrVG Rn. 18.

[1409] Altenburg, v. Reinersdorff, Leister, MMR 2005, 222, 223. In BAG AP Nr. 2 zu § 87 BetrVG 1972 „Ordnung des Betriebs“ wird darauf verwiesen, dass eine die betriebliche Ordnung betreffende Maßnahme beispielsweise vorliegt, wenn der Arbeitgeber zur Pünktlichkeitskontrolle Anwesenheitslisten führen lässt und anordnet, dass zu spät kommende Arbeitnehmer sich zur Eintragung in die Liste beim Listenführer melden müssen. Siehe zur betrieblichen Ordnung auch Worzalla in: Hess/Schlochauer/Worzalla/Glock, § 87 BetrVG Rn. 99; Matthes in: Münchener Handbuch Arbeitsrecht, § 333 Rn. 1. Siehe auch Fitting, Betriebsverfassungsgesetz, § 87 BetrVG Rn. 64 mit dem Hinweis, dass zur Ordnung des Betriebes allgemeingütige, verbindliche Verhaltensregeln zählen, die dazu dienen, das sonstige Verhalten der Arbeitnehmer zu beeinflussen und zu koordinieren. Vgl. zur Ordnung des Betriebs gemäß § 87 Abs. 1 Nr. 1 auch Bender in: Wlotzke/Preis, BetrVG, § 87 BetrVG Rn. 31.

[1410] Vgl. auch Fitting, Betriebsverfassungsgesetz, § 87 BetrVG Rn. 216 zum präventiven Schutzcharakter des Mitbestimmungsrechts des Betriebsrates gemäß § 87 Abs. Nr. 6 BetrVG.

der Arbeitnehmer durch technische Einrichtungen erfolgt.[1411]
Mitbestimmungspflichtig im Sinne von § 87 Abs. 1 Nr. 6 BetrVG sind technische Kontrolleinrichtungen dann, wenn sie zur Überwachung des Verhaltens der oder der Leistung von Arbeitnehmer objektiv und unmittelbar geeignet sind, ohne Rücksicht darauf, ob der Arbeitgeber dieses Ziel verfolgt und die durch die Überwachung gewonnenen Daten auswertet.[1412] Dieses Mitbestimmungsrecht kann im Übrigen bei Fällen einer praktisch permanenten Überwachung (wie sie

[1411] So Bantle in: Kittner/Zwanziger, Arbeitsrecht, § 113 Rn. 54; Fitting, Betriebsverfassungsgesetz, § 87 BetrVG Rn. 214. Auf den Meinungsstreit, ob es sich bei § 87 Abs. 1 Nr. 6 BetrVG um eine selbständige Regelung handelt, die § 87 Abs. 1 Nr. 1 BetrVG verdrängt, kommt es aber wegen der gerade getroffenen Feststellung nicht an. Auch das BAG prüft in einer Entscheidung § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG nebeneinander, ohne auf deren Verhältnis zueinander einzugehen. Siehe die Anmerkung von Wiese zu BAG AP Nr. 40 zu § 87 BetrVG 1972 „Überwachung". Wiese (aaO) verweist in seiner Anmerkung auf die h.M., wonach § 87 Abs. 1 Nr. 6 BetrVG eine selbständige Regelung enthält und die Anwendung des § 87 Abs. 1 Nr. 1 BetrVG ausschließt. Vgl. hierzu Wiese unter Verweis auf Fitting, Betriebsverfassungsgesetz, § 87 BetrVG Rn. 214; Galperin/Löwisch, Kommentar zum Betriebsverfassungsgesetz, § 87 BetrVG Rn. 59a; Moll, DB 1982, 1722, 1723; Moll, ZIP 1982, 889, 893; Ossberger, Betriebliche Kontrollen, ihre Voraussetzungen und Grenzen, S. 102/108; Schwarz, Arbeitnehmerüberwachung und Mitbestimmung, S. 92; Wiese, Das Initiativrecht nach dem Betriebsverfassungsgesetz, S. 50; Worzalla in: Hess/Schlochauer/Worzalla/Glock, § 87 BetrVG Rn. 287. Vgl. auch BAG AP Nr. 4 zu § 87 BetrVG1972 „Initiativrecht", wo ausgeführt wird, dass sich das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 1 BetrVG hinsichtlich der Gestaltung der betrieblichen Ordnung nicht auf die Einführung technischer Kontrolleinrichtungen erstrecke, da deren Mitbestimmungspflichtigkeit in § 87 Abs. 1 Nr. 6 BetrVG abschließend geregelt sei. Wiese verweist in seiner Anmerkung zu BAG AP Nr. 40 zu § 87 BetrVG 1972 „Überwachung" auch darauf, dass es nicht berechtigt ist, § 87 Abs. 1 Nr. 6 BetrVG gegenüber dessen Nr. 1 als Spezialvorschrift zu bezeichnen (so aber Fitting, Betriebsverfassungsgesetz, § 87 BetrVG Rn. 214), da nicht jede Überwachungsmaßnahme i.S.d. § 87 Abs. 1 Nr. 6 BetrVG zugleich die Ordnung des Betriebes und das Verhalten der Arbeitnehmer im Betrieb regelt (so beispielsweise die Datenverarbeitung).
[1412] BAG AP Nr. 2 zu § 87 BetrVG 1972 „Überwachung"; BAG AP Nr. 40 zu § 87 BetrVG 1972 „Überwachung"; Wedde, Telearbeit, S. 25/223; Altenburg/ v. Reinersdorff/ Leister, MMR 2005, 222, 223; Moll, ZIP 1982, 892, 894; Wedde, DuD 2004, 169, 173; Wedde, CR 1994, S. 230, 234; Däubler in: Ahrens/Donner/Simon, Arbeit-Umwelt, 2001, S. 1, 5; Worzalla in: Hess/Schlochauer/Worzalla/Glock, § 87 BetrVG Rn. 293; Bantle in: Kittner/Zwanziger, Arbeitsrecht, § 113 Rn. 54. Siehe zu den Voraussetzungen des § 87 Abs. 1 Nr. 6 BetrVG auch Kania in: Erfurter Kommentar, § 87 BetrVG Rn. 48 ff. Vgl. zur „objektiven Eignung" gemäß § 87 Abs. 1 Nr. 6 ebenso Bender in: Wlotzke/Preis, BetrVG, § 87 BetrVG Rn. 115. Siehe zum Mitbestimmungsrecht des Betriebsrates bei der Einführung von Betriebsdatenerfassungssystemen ebenso Rosenfelder, Lexikon des Betriebsverfassungsrecht, S. 63. Zu berücksichtigen ist jedoch, dass nicht jede Kontrolle oder Überwachung der Arbeitnehmer mitbestimmungspflichtig ist; das Mitbestimmungsrecht kommt erst zum Tragen, wenn die Kontrolle mit Hilfe technischer Einrichtungen erfolgt (Bantle in: Kittner/Zwanziger, Arbeitsrecht, § 113 Rn. 53). Klebe in: Däubler/Kittner/Klebe, BetrVG, § 87 BetrVG Rn. 137 verweist darauf, dass der Begriff der technischen Einrichtung weit zu fassen ist und hierunter alle optischen, akustischen, mechanischen und auch elektronischen Geräte zu verstehen. Siehe zu den Hilfsmitteln bei der Beobachtung von Menschen auch Worzalla in: Hess/Schlochauer/Worzalla/Glock, § 87 BetrVG Rn. 288.

durch Logdateien gegeben ist) auch nicht durch eine Einwilligung des betroffenen Arbeitnehmers ersetzt werden.[1413]

Sofern der Arbeitgeber also nicht das zusätzliche Ziel verfolgt, das „Internet-Verhalten“ seiner Mitarbeiter (im Sinne einer betrieblichen Ordnung) zu regeln, ergibt sich das Mitbestimmungsrecht des Betriebsrates ausschließlich aus § 87 Abs. 1 Nr. 6 BetrVG.

b. Datenvermeidung nach TKG

aa. Freiwilliges Tunneling

Beim freiwilligen Tunneling innerhalb eines VPN kann die Nutzung zu privaten Zwecken durch Arbeitnehmer anders als beim zwangsweisen Tunneling nicht allein aufgrund der Technik ausgeschlossen werden.
Etwas anderes ergibt sich nur im Rahmen des freiwilligen Tunneling und der privaten Internetnutzung, sofern der Nutzer selbständig entscheiden kann, ob ein Tunnel und wohin die Verbindung aufgebaut werden soll.
Hier liegt bei Bereitstellung des Internetzugangs im Verhältnis zwischen VPN-Auftraggeber und Mitarbeiter die Eigenschaft des Dritten gemäß § 3 Nr. 10 TKG vor, da der Mitarbeiter bei privater Internetnutzung nicht derart in den Betrieb eingegliedert ist, dass von der Identität des VPN-Auftraggebers und des Nutzers bzw. von einer Kommunikationseinheit ausgegangen werden kann.[1414]
Es handelt sich vielmehr um die eigene Kommunikation des jeweiligen Nutzers. Untersagt der Arbeitgeber die private Nutzung nicht ausdrücklich, so obliegen ihm Löschungspflichten bezüglich der anfallenden Verkehrsdaten gemäß §§ 96 ff. TKG.[1415] Die Verkehrsdaten fallen darüber hinaus unter das Fernmeldegeheimnis nach § 88 TKG.[1416] Bei einem Verstoß gegen das Fernmeldegeheimnis kommt zudem eine Strafbarkeit nach § 206 Abs. 1, Abs. 5

[1413] Vgl. Wedde, AuR 2005, 453, 458 zur Frage der Zulässigkeit der Videoüberwachung von Arbeitnehmern und unter Bezugnahme auf die Entscheidung des 1. Senats des BAG (BAG AuR 2005, 453, 454 ff.). Siehe zu den Beschlüssen des BAG bereits die Ausführungen auf S. 326.
[1414] Vgl. hierzu S. 320.
[1415] Siehe zur Anwendung des TKG im Arbeitsverhältnis Däubler, Gläserne Belegschaften?, Rn. 336, der ebenso zwischen privater und dienstlicher Kommunikation trennt. Beim freiwilligen Tunneling kommen im Übrigen die Regelungen des BDSG nicht zur Anwendung, da hier die vorrangigen Regelungen der §§ 91 ff. TKG gelten.
[1416] Dies gilt ebenso für den Inhalt der E-Mail, siehe Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 34.

S. 2 und 3 StGB sowie § 43 Abs. 2 BDSG i.V.m. § 44 BDSG in Betracht, wenn dem Arbeitnehmer die private Nutzung gestattet ist.[1417]

Zu weit geht die Auffassung, dass eine Protokollierung der Daten des zugreifenden Rechners nebst Datum und Uhrzeit sowie Adresse der aufgerufenen Website möglich sein soll.[1418]

Denn sofern die Daten nicht für Abrechnungszwecke erforderlich sind, sind sie unverzüglich nach der Beendigung der Verbindung gemäß § 96 Abs. 2 TKG zu löschen. Abrechnungszwecke kommen beispielsweise dann in Betracht, wenn der Arbeitgeber die Privatnutzung nur gegen Kostenerstattung erlaubt.[1419]

Insbesondere kann auch hier der Meinung nicht gefolgt werden, die ein Recht des Arbeitgebers zur Speicherung der Verbindungsdaten bejaht, um missbräuchliche Verwendung festzustellen.[1420]

Dies würde letztendlich eine Verhaltens- und Leistungskontrolle darstellen, die nur mit Einwilligung des Arbeitnehmers zulässig ist. Erst zu dem Zeitpunkt, zu welchem sich tatsächliche Anhaltspunkte gemäß § 100 Abs. 3 TKG ergeben, die außerdem dokumentiert werden müssen, darf der Arbeitgeber die entsprechenden Daten speichern. Der Diensteanbieter darf in diesem Rahmen einen Gesamtdatenbestand aus Verkehrsdaten und pseudonymisierten Bestandsdaten bilden (§ 100 Abs. 3 S. 3 TKG).[1421] Der Arbeitgeber darf demnach insgesamt erst dann kontrollieren und die Daten nutzen, wenn er einen konkreten Missbrauchsverdacht hat.[1422]

Des Weiteren kann sich ebenso eine längerfristige Speicherungsberechtigung aus § 100 Abs. 1 TKG ergeben. Auch hier muss wiederum geprüft werden, welcher Zeitraum für die Fehlerbehebung und Störungssuche erforderlich ist. Die Speicherdauer ergibt sich hier aus dem Kriterium der Erforderlichkeit, wobei eine abstrakte Regelung nicht sinnvoll wäre, da der Löschungszeitpunkt im

---

[1417] Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 138; Bier, DuD 2004, 277, 278; Bizer, DuD 2004, 432, 432; Weißnicht, MMR 2003, 448, 451.

[1418] Ueckert, ITRB 2003, 158, 160; Altenburg/v. Reinersdorff/Leister; MMR 2005, 135, 136.

[1419] Vgl. auch Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 137; Mengel, BB 2004, 1445, 1448/1449.

[1420] Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 49.

[1421] Vgl. Ohlenburg, MMR 2004, 431, 437.

[1422] Vgl. auch Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 32, der darauf verweist, dass eine vollständige Überwachung und Aufzeichnung der Telekommunikationsinhalte ohne konkreten Anlass eines Missbrauchs das Recht des Arbeitnehmers auf informationelle Selbstbestimmung verletzt. Im Übrigen müssen Kontrollverfahren nicht nur zweck- oder anlassbezogen und verhältnismäßig sein, sondern dem Arbeitnehmer auch bekannt sein (Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 31). Ebenso Rosen, The unwanted gaze, The destruction of privacy in America, S. 72 ff.

Einzelfall unterschiedlich sein kann.[1423] So können für Zwecke der Störungssuche zwei Wochen ausreichend sein.[1424] Für Zwecke der Abrechnung oder aber Aufdeckung von Missbräuchen kann jedoch ein längerer Zeitraum in Betracht kommen, wobei hier auf die Ausführungen zum Access-Providing verwiesen werden kann.[1425]
Diesbezüglich kann sich auch für ein Arbeitsverhältnis keine andere Bewertung ergeben. Denn sofern Datenschutz auch im Arbeitsverhältnis bei privater Internetnutzung Anwendung finden soll, sind keine Gründe ersichtlich, warum auf der anderen Seite wieder Ausnahmen von den gesetzlichen Vorschriften geschaffen werden sollen. Insbesondere ist zu berücksichtigen, dass diese Daten nicht zur Verhaltens- und Leistungskontrolle genutzt werden dürfen.[1426] Dies bedeutet, dass der Arbeitgeber selbst bei einer ausschließlich dienstlichen Nutzung des Internetzugangs nur eingeschränkte Kontrollmöglichkeiten hat. Daher muss dies erst recht bei einer erlaubten privaten Internetnutzung gelten.

bb. Nutzungsdetails

Bezüglich dieses Prüfungspunktes muss zunächst auf die Ergebnisse eines anderen Personenverhältnisses zurückgegriffen werden: Aus den rechtlichen Ausführungen zum Personenverhältnis „Provider/Nutzer“ ergibt sich, dass der Arbeitgeber einer separaten Einwilligung der Arbeitnehmer gemäß § 4a BDSG bedarf, sofern er technische Einrichtungen einsetzen möchte, die das Nutzungsverhalten der Arbeitnehmer registrieren.[1427]
So verlangt § 99 Abs. 1 S. 2 TKG, dass der Teilnehmer die Nutzer bezüglich des Einzelverbindungsnachweises informiert hat, wobei es sich um eine Datenschutzregel zugunsten der Nutzer handelt. Auch Domain-Namen fallen seit der Gesetzesnovellierung des TKG unter den Begriff der Nummern gemäß § 3 Nr. 13 TKG,[1428] so dass sich ein Einzelverbindungsnachweis ebenso (zusätzlich) auf dieses Datum beziehen könnte. Im Hinblick auf die Gesamtnutzungsdaten der Kommunikation ist jedoch die Feststellung wichtig,

---

[1423] Vgl. Ohlenburg, MMR 2004, 431, 437.
[1424] Gerling, DuD 2005, 338, 339. Siehe auch S. 324.
[1425] Siehe die obigen Ausführungen auf S. 177 ff.
[1426] So Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 79 sowie oben S. 320 ff.
[1427] Siehe S. 281 ff. Vgl. auch Mengel, BB 2004, 1445,1451 zur Kontrolle der Zielrufnummer bei Arbeitnehmern, denen die Nutzung der betrieblichen Telefonanlage kostenpflichtig gestattet ist.
[1428] Siehe S. 188.

dass es sich insgesamt um private Kommunikation handelt und damit das Fernmeldegeheimnis des Nutzers bzw. Arbeitnehmers gemäß § 88 TKG betroffen ist. Damit ist nicht nur im Sinne von § 99 Abs. 1 S. 2 TKG die Information der Nutzer ausreichend, sondern darüber hinausgehend zu verlangen, dass der Nutzer seine Einwilligung gemäß § 4a BDSG erteilt hat.[1429] Diese Einwilligung muss außerdem für die Zukunft frei widerruflich sein, da diesbezüglich ein faktischer Druck des Arbeitgebers auf den Nutzer bzw. Arbeitnehmer in Betracht kommen könnte, und dieser sich gegebenenfalls dem Willen seines Arbeitgebers ungern entziehen möchte.[1430]
Die in § 99 TKG vom Teilnehmer geforderte Erklärung, dass er Mitbenutzer (Mitarbeiter) über die Bereitstellung des Einzelverbindungsnachweises informiert hat, zukünftige informieren wird und er außerdem den Betriebsrat beteiligt hat, ist daher verbesserungsbedürftig.[1431] In rechtspolitischer Hinsicht hätte in § 99 TKG eine Unterteilung in dienstliche und private Kommunikation stattfinden müssen. Denn nur in Bezug auf die dienstliche Kommunikation reicht seitens eines Teilnehmers die Information der Nutzer aus. Bei privater Kommunikation der „Mitbenutzer“ sollte die Information durch eine Einwilligung gemäß § 4a BDSG ersetzt werden. Daher müsste der Teilnehmer gemäß § 99 Abs. 1 S. 2 TKG erklären, dass der Nutzer in die Übersicht der Nutzungsdetails eingewilligt oder der Betriebsrat ausdrücklich erklärt hat, dass keine Bedenken gegen die Einführung eines Einzelverbindungsnachweises bestehen. Aus Gründen der Vereinfachung hätte in § 99 TKG aber auch für beide Varianten die Erklärung einer Einwilligung enthalten sein können anstatt einer „bloßen“ Information.

Insbesondere ist in diesem Zusammenhang zu beachten, dass Standortdaten,[1432] die besonders bei mobiler Einwahl des Nutzers mittels des

[1429] § 3 Abs. 3 TDSV hat im neuen TKG keine entsprechende Integration gefunden, so dass auf die allgemeinen datenschutzrechtlichen Regelungen zurückzugreifen ist. Hiervon unberührt bleibt jedoch die Möglichkeit der Einwilligung im elektronischen Verfahren gemäß § 94 TKG.
[1430] Siehe hierzu auch die folgenden Ausführungen auf S. 363 insbesondere Fn. 1563/1564. Siehe zur Freiwilligkeit Däubler, Internet und Arbeitsrecht, Rn. 332a; Däubler, Gläserne Belegschaften?, Rn. 150 ff. Vgl. im Übrigen Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 288 zur Widerrufsmöglichkeit des TDDSG, der anmerkt, dass die jederzeitige Widerrufsmöglichkeit der Einwilligung Ausdruck der Entscheidungsfreiheit des Nutzers über die Verwendung seiner Daten ist, wobei sie den Nutzer gleichzeitig vor einer überholt getroffenen Entscheidung schützen soll.
[1431] Vgl. hierzu bereits die Ausführungen auf S. 281 ff.
[1432] Siehe zum Begriff der Standortdaten S. 99 ff.

Firmen-Rechners oder Firmen-Handys anfallen können, für die volumenmäßige Abrechnung ebenso Relevanz haben können. Denn sofern die Einwahl etwa aus dem Ausland kostenintensiver ist, hätte der Arbeitgeber diesbezüglich ein Interesse daran zu erfahren, von welchen Standorten aus die Einwahl erfolgt ist. Daher muss sich die Einwilligung des Nutzers auch auf die Verarbeitung seiner Standortdaten beziehen.[1433]

2. VPN-Kommunikation

Die VPN-Nutzung führt zu einer geschlossenen Benutzergruppe, da zum einen die unter den Beteiligten geführte Kommunikation durch die Vergabe entsprechender Zugriffsberechtigungen und Authentifizierungsverfahren lediglich zwischen den hierzu legitimierten Stellen stattfindet.
Zum anderen werden identische berufliche und/oder wirtschaftliche Ziele verfolgt.[1434] So können alle durch Lieferanten- oder Kundenbeziehungen verbundenen Unternehmen eine geschlossene Benutzergruppe bilden.[1435] Damit sind sowohl die Mitarbeiter des VPN-Auftraggebers als auch externe zugriffsberechtigte Personen (etwa Lieferanten) durch die Bereitstellung der „privaten Leitungen“, die ein Arbeiten „wie im Büro nebenan“ ermöglichen können,[1436] miteinander verbunden. Die Mitglieder des VPN als geschlossene Benutzergruppe lassen sich insgesamt anhand abstrakter Kriterien ermitteln und, insbesondere durch die eingeschränkten Zugriffsberechtigungen, von der Öffentlichkeit unterscheiden.[1437]

Nachfolgend sollen die datenschutzrechtlichen Pflichten im Hinblick auf die unterschiedlichen technischen Systeme eines VPN (Unternehmensserver und Gateway) im Rahmen einer solchen geschlossenen Benutzergruppe untersucht

[1433] Siehe auch Wedde, RDV 1996, 5, 8/9, der anmerkt, dass mittels des Firmen-Handys und eines Einzelgebührennachweises der Arbeitgeber leicht eine Verhaltens- und Leistungskontrolle des Mitarbeiters durchführen könnte.
[1434] Siehe zur geschlossenen Benutzergruppe ebenso die Ausführungen auf S. 184 ff. Auch bei geschlossenen Benutzergruppen finden die datenschutzrechtlichen Regelungen der §§ 91 ff. TKG grundsätzlich Anwendung, sofern dies nicht ausdrücklich eingeschränkt ist.
[1435] Vgl. zum Begriff der geschlossenen Benutzergruppe auch Manssen in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 3 TKG(1998), Band 1, Rn. 39.
[1436] Siehe die Ausführungen in der Einführung S. 2.
[1437] Vgl. hierzu Zimmer, CR 2003, 893, 894.

werden.[1438] Zu berücksichtigen ist hierbei, dass es sich bei der VPN-Kommunikation zum einen um einen Telekommunikationsdienst handeln kann, was dann in Betracht kommt, wenn den Nutzern die Möglichkeit bereitgestellt wird, „ihre“ oder die von ihnen be- und erarbeiteten Daten auf den Firmenserver zu übertragen.[1439] Zum anderen kommt ein Teledienst in Betracht, wenn die Nutzer Daten vom Firmenserver abrufen können.[1440]
Ein VPN-Auftraggeber wird aber seinen Nutzern oftmals beide Möglichkeiten zur Verfügung stellen wollen, so dass zu prüfen ist, wie die datenschutzrechtlichen Anforderungen an das konkrete technische System (den Unternehmensserver) in diesem Falle aussehen.

Die nachfolgenden Ausführungen unterscheiden nach diesen drei Möglichkeiten, wobei zunächst die Verpflichtung des VPN-Auftraggebers zur Datenvermeidung bezüglich der auf einem Unternehmensserver entstehenden Protokolldaten untersucht wird.

a. Unternehmensserver

Auf dem Server[1441] in der Unternehmenszentrale, auf den der Nutzer beim Datentransport Zugriff nimmt, werden regelmäßig Daten protokolliert, die sich auf Datum, Uhrzeit, verwendetes Protokoll oder Länge des Datenpakets beziehen. Daher stellt sich die Frage nach der Löschungspflicht dieser Daten.

aa. Datenvermeidung

aaa. Telekommunikationsdienst

Oben wurde festgestellt, dass der Server in der Firmenzentrale sowohl beim Software-VPN als auch beim Gateway-VPN für Zwecke der Telekommunikation

[1438] Siehe zu den datenschutzrechtlichen Pflichten das Prüfungsschema auf S. 106 ff.
[1439] Siehe zu dieser Unterscheidung die obigen Ausführungen auf S. 312 ff.
[1440] Vgl. hierzu die Ausführungen auf S. 310 ff.
[1441] Gemeint ist hier der Server, auf welchem die inhaltlichen Daten gespeichert sind, auf die der Nutzer Zugriff nehmen möchte. Auch auf dem Web-Server wird die Anfrage des Nutzers in einer Logdatei gespeichert (siehe auch: Roßnagel, Datenschutz beim Online-Einkauf, S. 41; Köhntopp/Köhntopp, CR 2000, 248, 251, wobei sich im Rahmen eines VPN jedoch die Besonderheit ergibt, dass der Web-Server hier keinem Dritten, sondern dem VPN-Auftraggeber „gehört“.).

gemäß § 3 Nr. 22 TKG zur Verfügung stehen kann,so dass ein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG vorliegt.[1442] Gemeint ist hiermit zum einen die Möglichkeit Nutzer, Daten im VPN selbständig zu übertragen und auf dem Server abzulegen, sowie zum anderen die Funktion des Servers beim Software-VPN in der Firmenzentrale als Kommunikationsplattform.

Die datenschutzrechtlichen Regelungen der §§ 91 ff. TKG kommen allerdings nur in Betracht, sofern es sich um ein geschäftsmäßiges Handeln und damit um das nachhaltige Angebot von Telekommunikation gemäß § 3 Nr. 10 TKG *an Dritte* handelt. Daher wird im Folgenden untersucht, inwieweit im Verhältnis zwischen VPN-Auftraggeber und Nutzer „geschäftsmäßiges Handeln" gemäß § 91 TKG in Betracht kommen kann.

(1) Anwendbarkeit des BDSG bei gemeinsamer Zweckverfolgung der Nutzer

Fraglich ist, ob allein die Einstufung als geschlossene Benutzergruppe ausreichen könnte, um ein geschäftsmäßiges Handeln gemäß § 91 TKG abzulehnen. Dies ist jedoch zu verneinen, da grundsätzlich *auch Dritte* in eine geschlossene Benutzergruppe integriert sein können. Dies ergibt sich aus dem Wortlaut §§ 91 ff. TKG, da stets – ebenso im Rahmen einer geschlossenen Benutzergruppe - vorausgesetzt wird, dass der Telekommunikationsdienst geschäftsmäßig, d.h. für Dritte erbracht wird. [1443] Damit können ebenso Dritte Mitglieder einer geschlossenen Benutzergruppe sein, die dadurch gekennzeichnet ist, dass ihre Teilnehmer in gesellschaftsrechtlichen oder schuldrechtlichen Dauerbeziehungen oder sonstigen nicht-vertraglichen, aber dauerhaften Verbindungen zur Verfolgung gemeinsamer beruflicher, wirtschaftlicher oder hoheitlicher Ziele stehen.[1444]

Für die Bejahung oder Ablehnung von *geschäftsmäßigem Handeln* ist daher das Merkmal des Dritten gemäß § 3 Nr. 10 TKG und die Frage entscheidend,

[1442] Vgl. hierzu die Ausführungen auf S. 312 ff.
[1443] Vgl. hierzu auch Gola, MMR 1999, 321, 324, Gola/Klug, Grundzüge des Datenschutzrechts, S. 198.
[1444] Vgl. hierzu S. 335. Vgl. Schütz in: TKG-Kommentar (2. Auflage), § 3 TKG Rn. 22; Schütz in: TKG-Kommentar (3. Auflage), § 6 TKG Fn. 62; Trute/Spoerr/Bosch, TKG-Kommentar, § 3 TKG Rn. 85; Manssen in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 3 TKG(1998), Band 1, Rn. 39; vgl. auch § 6 Abs. 2 Telekommunikations-Verleihungsverordnung.

ob die zugriffsberechtigten Personen in einem VPN in den Betriebsablauf eingegliedert sind.[1445] Hier hilft der Rückgriff auf § 3 Abs. 8 BDSG, in dem das Merkmal des Dritten definiert ist und damit jede natürliche oder juristische Person außerhalb der verantwortlichen Stelle bezeichnet wird.[1446]
Diesbezüglich wird die Auffassung vertreten, dass im Sinne von § 3 Abs. 8 BDSG **jede** natürliche oder juristische Person oder Gesellschaft eine verantwortliche Stelle ist und **jede andere** natürliche oder juristische Person oder Gesellschaft im Verhältnis zu ihr die Eigenschaft des Dritten erfüllt.[1447]
Allerdings ist zu berücksichtigen, dass diese Auslegung aus der Sicht eines Betroffenen erfolgt, dessen Daten verarbeitet werden.
In dem hier untersuchten Personenverhältnis „VPN-Auftraggeber/Nutzer" ist für das Merkmal des „Dritten" und des „geschäftsmäßiges Handeln" eine Sichtweise aus diesem Innenverhältnis heraus sowie die gemeinsame Zweckverfolgung entscheidend. Insoweit kann eine Parallele zum TDDSG gezogen werden, welches die datenschutzrechtlichen Belange zwischen einem Diensteanbieter und einem Nutzer regelt. So ist in § 1 Abs. 1 S. 2 Nr. 1 und Nr. 2 TDDSG ausdrücklich geregelt, dass datenschutzrechtliche Regelungen im Hinblick auf die Nutzung von Telediensten zu ausschließlich beruflichen oder dienstlichen Zwecken oder innerhalb von Unternehmen zur ausschließlichen Steuerung von Arbeits- und Geschäftsprozessen keine Anwendung finden. Dieses Verständnis ist ebenso bei der Auslegung des geschäftsmäßigen Handelns gemäß § 91 TKG zugrunde zu legen. Unabhängig davon, ob nun Mitarbeitern oder Externen (Lieferanten) Zugriff auf das VPN gewährt wird, sind diese bei Verfolgung von gemeinsamen Interessen und identischen Zwecken (etwa die gemeinsame Erledigung und Förderung der Bearbeitung eines Auftrages) derart untereinander verbunden, dass eine Einordnung als Dritter gemäß § 3 Nr. 10 TKG nicht in Betracht kommt.[1448] Es handelt sich in diesem Falle um rein interne Kommunikation zur beruflichen und geschäftlichen „Eigennutzung" innerhalb eines VPN und nicht um Angebot und Nachfrage.[1449]

[1445] Vgl. hierzu S. 320 ff.
[1446] Vgl. Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 230/232.
[1447] Vgl. Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 232. Siehe zum Begriff des Dritten auch Gola/Schomerus, BDSG, § 3 BDSG Rn. 52.
[1448] Vgl. oben S. 320 ff. und Gola, MMR 1999, 322, 325; Gola/Klug, Grundzüge des Datenschutzrechts, S. 198; Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 75.
[1449] Vgl. auch Gola, MMR 1999, 321, 328.

Der Nutzer steht in diesem Falle der gemeinsamen Zweckverfolgung nicht außerhalb „des Betriebs“ und der Kommunikationseinheit.. In diesem Zusammenhang ist ebenso unerheblich, ob es sich um einen Telearbeiter, den Nutzer innerhalb einer Zweigstelle oder einen Lieferanten handelt, und ob er von den Weisungen des VPN-Auftraggebers abhängig ist. Entscheidend ist **in dem hier untersuchten** Personenverhältnis allein das Innenverhältnis zwischen Nutzer und der VPN-Auftraggeber, die identische Zwecke verfolgen. Damit ist der Nutzer kein Dritter.

Eine andere Auslegung im Hinblick auf das Merkmal des Dritten kann sich allenfalls im Personenverhältnis „Nutzer/Betroffener“ ergeben, da in diesen Personenverhältnissen die Sicht des Betroffenen entscheidend ist. Werden seine Daten zur Bearbeitung des Auftrags weitergegeben, liegt aus seiner Sicht eine Funktionsübertragung und die Eigenschaft eines Dritten in dem Falle vor, wenn der VPN-Auftraggeber oder der Nutzer (jeweils) ein eigenständiges Interesse an dem Geschäft haben und seine Daten (jeweils) für eigene Geschäftszwecke verwenden.[1450]
Daher zeigt sich an dieser Stelle wiederum, dass die Gesamtbetrachtung der Personenverhältnisse erforderlich ist und außerdem der Verwendungszweck Einfluss auf Begriffsdefinitionen haben kann.

Der VPN-Auftraggeber erbringt somit weder im Rahmen eines Software-VPN (durch die hier erfolgte Bereitstellung eines Servers als Kommunikationsmöglichkeit[1451]) noch durch das Bereithalten eines Servers (mit der Möglichkeit, Daten dort abzulegen bzw. auf diesen zu übertragen[1452]) einen geschäftsmäßigen Telekommunikationsdienst gegenüber den Nutzern, da diese Personen keine Dritten gemäß § 3 Nr. 10 TKG darstellen. Dementsprechend richten sich die datenschutzrechtlichen Pflichten nicht nach §§ 91 ff. TKG bzw.

[1450] Siehe hierzu die Ausführungen auf S. 448 ff.
[1451] Vgl. hierzu die Ausführungen auf S. 312 ff. sowie Fn. 9 und das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch“, S. 14, wo ausgeführt wird, dass ein Benutzer nach der erfolgreichen Anmeldung am directVPN mit anderen angemeldeten Computern Daten austauschen kann.
[1452] Siehe ebenso die Ausführungen auf S. 312 ff.

§§ 96 ff. TKG, sondern nach dem BDSG.[1453] Die Anwendung des BDSG wird hier insbesondere nicht durch das TKG ausgeschlossen. §§ 91 ff. TKG beinhalten im Verhältnis zum BDSG vorrangige Regelungen, sofern das *geschäftsmäßige* Erbringen von Telekommunikationsdiensten Gegenstand der Betrachtung ist. , In §§ 91 ff. TKG finden sich jedoch keine Regelungen bezüglich des datenschutzrechtlichen Umgangs mit personenbezogenen Daten, die „nur" im Zusammenhang mit Telekommunikationsdiensten gemäß § 3 Nr. 24 TKG anfallen, die *nicht geschäftsmäßig* erbracht werden.

Daher muss auch hier die umfassende Protokollierung von Zugriffszeiten, Datum und abgerufenen Inhalten im Sinne von § 28 Abs. 1 Nr. 1 BDSG[1454] zulässig sein, jedoch unter der Einschränkung, dass diese nicht zur Verhaltens- oder Leistungskontrolle der Mitarbeiter[1455] gebraucht werden darf, sondern allein zur Gewährleistung eines ordnungsgemäßen Betriebs.[1456] Hieraus folgt eine enge Zweckbindung der Daten. Dies hat gleichermaßen eine technische Komponente, da die Sicherheit und der Betrieb der Systeme gewährleistet sein muss.

Die Löschungspflichten richten sich infolgedessen ebenso nach § 35 Abs. 2 BDSG. Dabei obliegt dem VPN-Auftraggeber ein regelmäßiges Prüfungsrecht, für welchen Zeitraum er die Protokolle benötigt, so dass diese gemäß § 35 Abs. 2 Nr. 3 BDSG zu löschen sind, sofern ihr ursprünglicher Speicherungszweck weggefallen ist und sich auch im Rahmen des Arbeitsverhältnisses kein erneuter Zweck herausgebildet hat, der eine längerfristige Speicherung rechtfertigen könnte.[1457]

[1453] Zum Charakter des BDSG als Auffanggesetz siehe auch Schaffland/Wiltfang, BDSG, § 1 BDSG Rn. 37. Zum Exklusivitätsverhältnis siehe S. 92.

[1454] Das TKG kommt hier nicht zur Anwendung, da der Mitarbeiter kein Dritter im Sinne von § 3 Nr. 10 TKG ist, siehe oben S. 320 ff.

[1455] Vgl. Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 82; vgl. außerdem v.Zezschwitz in: Roßnagel, Handbuch Datenschutzrecht, 1 Rn. 42. Vgl. auch Mengel, BB 2004, 2014, 2020, die von einer umfassenden Kontrollbefugnis ausgeht.

[1456] Vgl. hierzu oben S. 320 ff. Vgl. außerdem für den E-Mail-Verkehr Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 77 und der Ausführung, dass der Anwendungsbereich des BDSG dann nicht eröffnet ist und keine Übermittlung an Dritte im Sinne von § 3 Abs. 5 Nr. 3 BDSG vorliegt, wenn die E-Mails den Unternehmensbereich nicht verlassen.

[1457] Siehe die Ausführungen zum Internetzugang auf S. 324. Vgl. außerdem Fn. 908 unter Verweis auf Gola/Schomerus, BDSG, § 35 BDSG Rn. 13. Siehe auch die Ausführungen von Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 27.

(2) Anwendbarkeit des TKG bei eigenen Zwecken der Nutzer

Etwas anderes kann sich jedoch für ein Extranet-VPN ergeben.[1458] Sofern beispielsweise der zugriffsberechtigte Lieferant oder Kunde des VPN-Auftraggebers eigene Zwecke verfolgt kann er nicht mehr als Teil der Kommunikationseinheit gewertet werden und ist damit Dritter gemäß § 3 Nr. 10 TKG.[1459]
So wäre vorstellbar, dass der VPN-Auftraggeber seinem Kunden oder Lieferanten eine Zugriffsberechtigung auf sein Firmennetz gewährt, damit dieser eigene personenbezogene Daten auf den Server übertragen kann, ohne dass ein gemeinsamer Zweck oder identisches Ziel feststellbar wäre.[1460]
Erhält beispielsweise ein ausgesuchter Kundenkreis Zugriffsrechte auf das VPN und den Firmenserver, um dort Bestelldaten gesichert anzugeben, dann werden vorrangig eigene Zwecke verfolgt und die Kunden stehen insoweit außerhalb der verantwortlichen Stelle. Im Hinblick auf die Datenverarbeitung liegt dann grundsätzlich Schutzbedürftigkeit vor. Ähnliches gilt für die Datenübertragungen im Bankenbereich, bei dem ebenso VPN eingesetzt werden.[1461]

Auch ist möglich, dass der VPN-Auftraggeber innerhalb des VPN einem rechtlich selbständigen Tochterunternehmen (gegebenenfalls gegen Entgelt) die Möglichkeit anbietet, täglich seine Daten im Wege des Online-Backup-Verfahrens[1462] auf den Servern des VPN-Auftraggebers zu hosten. Im Rahmen dieser Fallgestaltung soll die Möglichkeit des VPN-Auftraggebers ausgeschlossen sein, diese Daten für eigene oder gemeinsame Zwecke nutzen

[1458] Siehe zum Begriff des Extranet-VPN S. 2 unter Verweis auf Lipp, VPN, S. 43; Buckbesch/Köhler, Virtuelle Private Netze, S. 16.
[1459] Siehe zur Kommunikationseinheit S. 320.
[1460] Siehe hierzu insbesondere auch die folgenden Ausführungen auf S. 345 ff.
[1461] Siehe oben Fn. 4 und dem Hinweis auf den Beitrag in der Frankfurter Allgemeinen Zeitung vom 23.08.2004, S. 17, wo darauf verwiesen worden ist, dass Schweizer Banken mit Virtuellen Privaten Netzwerken arbeiten.
[1462] Siehe zum Online-Backup-Verfahren S. 74/82. Zum Begriff des Hosting siehe S. 75 Fn. 313 unter Verweis unter anderem auf Geis, Recht im eCommerce, S.109; Härting, CR 2001, 37, 37/39; Pelz in: Bräutigam/Leupold, B I. Rn. 44; Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 12; Röhrborn/Sinhart, CR 2001, 69, 73; Cichon, Internetverträge,Rn. 160; Schuppert in: Spindler, Vertragsrecht der Internet Provider, Teil V Rn. 15 ff.; Komarnicki in: Hoeren/Sieber, Teil 12.2 Rn. 4; Pankoke, Von der Presse- zur Providerhaftung, S. 170.

zu dürfen.[1463] Insbesondere kann dem VPN-Auftraggeber ebenso ein eigenes Interesse unterstellt werden, welches im Falle des entgeltlichen Hosting von Gewinnerzielungsabsicht geprägt ist.

Hier kommen daher nicht zwangsläufig *ausschließlich gemeinsame* berufliche Interessen in Betracht. In diesem Falle handelt sich trotz der eingeschränkten Zugriffsberechtigungen auf den Server in der Firmenzentrale und der damit weiterhin zu bejahenden geschlossenen Benutzergruppe nicht mehr um eine Kommunikationseinheit. VPN-Auftraggeber und Nutzer verfolgen vorrangig jeweils eigene Zwecke.
Dementsprechend bietet der VPN-Auftraggeber den Nutzern nicht nur einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG,[1464] sondern darüber hinaus einen geschäftsmäßigen Telekommunikationsdienst gemäß § 3 Nr. 6 a) TKG in Verbindung mit §§ 91 ff. TKG an. Der Nutzer ist nicht derart mit dem VPN-Auftraggeber verbunden ist, dass eine einheitliche Zweckverfolgung unterstellt werden könnte. Dies gilt, auch wenn auf das Firmennetz und den Firmenserver des VPN-Auftraggebers nach wie vor lediglich unter der Voraussetzung der Authentifizierung durch den Nutzer zugegriffen werden kann, und sich die Leitungen „wie private“ darstellen.[1465]
Das VPN im technischen Sinne und als geschlossene Benutzergruppe ist daher von der Frage abzugrenzen, inwieweit *darüber hinaus* eine identische Zweckverfolgung in dem Sinne in Betracht kommt, dass das Merkmal des Dritten gemäß § 3 Nr. 10 TKG ausscheiden muss.

Dies bedeutet, dass in diesem Falle die erstellten Protokolle gemäß §§ 96 ff. TKG zu löschen sind, und zwar gemäß § 96 Abs. 2 TKG unverzüglich nach Ende der Verbindung, sofern sich nicht aus den Regelungen der §§ 97, 99 und 100 TKG ergibt. Insbesondere kann eine länger andauernde Speicherung aufgrund eines konkreten Missbrauchsverdachts im Sinne von

[1463] Siehe zum gegenteiligen Fall und zur Zulässigkeit eines konzerninternen Datenaustausches Däubler, Gläserne Belegschaften?, Rn. 450 ff.; Däubler, Internet und Arbeitsrecht, Rn. 335 ff.; Simitis in: Simitis, BDSG-Kommentar,§ 28 BDSG Rn. 211 ff.
[1464] Vgl. hierzu bereits die Ausführungen auf S. 312 ff.
[1465] Siehe die Ausführungen in der Einführung S. 2.

§ 100 Abs. 3 TKG in Betracht kommen, wobei hier aber die tatsächlichen Anhaltspunkte zu dokumentieren sind.[1466]

bbb. Teledienst

Bei der Bereitstellung eines *reinen* Abrufverfahrens auf dem Server der Firmenzentrale und der Bereitstellung von Informationen (ohne dem Nutzer die Möglichkeit der eigenständigen Datenübertragung zu eröffnen) ist gemäß § 2 Abs. 2 Nr. 1 TDG ein Teledienst gegeben.[1467] Es stehen eindeutig die Dateninhalte im Vordergrund, und der Zugriff erfolgt auf den nicht anwendungsdiensteunabhängig und nicht unabhängig von den Inhalten.[1468]

Gemäß § 1 Abs. 1 S. 2 Nr. 1 und Nr. 2 TDDSG ist in den Fällen, die hier aufgrund der Verfolgung gemeinsamer Zwecke als Kommunikationseinheit bezeichnet werden, die Anwendung von datenschutzrechtlichen Regelungen hingegen ausdrücklich ausgeschlossen. Daher ist fraglich, ob auf die Vorschriften des § 28 BDSG zurückgegriffen werden darf. Konsequenz wäre bei entsprechender Ablehnung der Anwendbarkeit von § 28 BDSG, dass der VPN-Auftraggeber umfassend auf seinem Server die Zugriffe protokollieren dürfte.[1469] Er könnte diese Protokolle dementsprechend ebenso zur Verhaltens- und Leistungskontrolle nutzen. Denn diese Protokollierung ist abgelehnt worden, da sie weder gemäß § 28 Abs. 1 Nr. 1 BDSG für den Zugriff auf den Server unabdingbar notwendig ist, noch die Interessen der Nutzer gemäß § 28 Abs. 1 Nr. 2 BDSG gegen eine solche Kontrolle sprechen. Kommen hingegen die einschränkenden Voraussetzungen des § 28 Abs. 1 BDSG von vorneherein nicht in Betracht, so kann eine umfassende Protokollierung stattfinden.[1470]

[1466] Siehe zum typischen Missbrauchsfall der Leistungserschleichung und dem Erfordernis, dass die tatsächlichen Anhaltspunkte konkret und einen dringenden Tatverdacht nahe legen müssen Büchner in: TKG-Kommentar (2. Auflage), § 7 TDSV (Anh § 89 TKG) Rn. 2; siehe zum konkreten Tatverdacht ebenso Wittern in: TKG-Kommentar (3. Auflage), § 100 TKG Rn. 9. Vgl. auch Gramlich in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 89 TKG(1998), Band 1, Rn. 76 ff.

[1467] Vgl. hierzu die Ausführungen auf S. 310 ff.

[1468] Siehe zum Begriff „anwendungsdiensteunabhängig“ S. 126.

[1469] Auch auf dem Web-Server wird die Anfrage des Nutzers in einer Logdatei gespeichert, siehe Roßnagel, Datenschutz beim Online-Einkauf, S. 41; Köhntopp/Köhntopp, CR 2000, 248, 251.

[1470] Siehe oben S. 321 ff.

Zu berücksichtigen ist allerdings, dass die Regelung des § 1 Abs. 1 S. 2 Nr. 1 und Nr. 2 TDDSG lediglich klarstellen sollte, dass das TDDSG nicht zur Anwendung gelangen soll, sofern es sich nicht um ein „öffentliches“ Angebot-Nutzer-Verhältnis handelt.[1471] Damit ist aber noch keine Spezialregelung bezüglich der Anwendbarkeit des BDSG getroffen worden. Da insbesondere bereits vor Einführung dieses Zusatzes die Regelungen des BDSG für die Prüfung der Zulässigkeit der Protokollierung im Arbeitsverhältnis Anwendung gefunden haben,[1472] gilt hier die oben entwickelte Lösung entsprechend.
Demnach muss der VPN-Auftraggeber § 28 Abs. 1 Nr. 1 oder Nr. 2 BDSG berücksichtigen und hat die entsprechenden Protokolle gemäß § 35 Abs. 2 Nr. 3 BDSG zu löschen, sofern er diese nicht mehr benötigt.[1473]

ccc. VPN als kombinierter Telekommunikations- und Teledienst

Regelmäßig wird der VPN-Auftraggeber seinen Nutzern die Möglichkeit des Datenabrufs sowie der Datenübertragung bereitstellen wollen. Dies kommt insbesondere in Betracht, sofern er seinen Mitarbeitern die Möglichkeit anbieten möchte, dass diese von ihrem häuslichen Bereich Zugriff auf den Firmenserver nehmen können, um ihre Arbeit zu erledigen.
Sofern der VPN-Auftraggeber keine getrennten Systeme hierfür bereitstellt, müsste sich die Datenvermeidung insgesamt nach der „strengsten“ Lösung richten. Da aber bei gemeinsamer Zweckverfolgung und unabhängig davon, ob es sich um einen Telekommunikationsdienst oder Teledienst handelt, insgesamt die Regelungen des BDSG Anwendung finden, muss der VPN-Auftraggeber dementsprechend die Prüfung an den Grundsätzen des § 35 Abs. 2 BDSG vornehmen. Hierbei ist daher die Datenaufbewahrung am Grundsatz der Erforderlichkeit zu messen.[1474]
Lediglich in den Fällen, in denen der Nutzer bei der Datenübertragung eigene Zwecke verfolgt, und damit außerhalb der Kommunikationseinheit steht,

[1471] Vgl. Büllesbach, DuD 1999, 263, 263.
[1472] Siehe etwa Post-Ortmann, RDV 1999, 102, 105.
[1473] Siehe die Ausführungen auf S. 324.
[1474] Siehe zur Erforderlichkeit im Rahmen von § 35 Abs. 2 BDSG die Ausführungen auf S. 229/299/324/340.

kommen die Anwendbarkeit des TKG und die dortigen Löschungsregelungen im Hinblick auf die Protokolldaten in Betracht.

Hier muss in technischer Hinsicht entschieden werden, ob eine getrennte Protokollierung der Daten auf dem Server erfolgen kann. Sofern dies nicht möglich ist, muss sich die Löschung der Daten insgesamt nach den strengsten datenschutzrechtlichen Regelungen richten, also unter Umständen gemäß § 96 Abs. 2 TKG eine unverzügliche Löschung der Daten erfolgen, soweit nicht eine längere Speicherung für Störungszwecke gemäß § 100 Abs. 1 TKG oder Missbrauchszwecke gemäß § 100 Abs. 3 TKG erforderlich ist. Bezüglich der Frage der Erforderlichkeit und der unverzüglichen Löschung der Daten gelten die obigen Ausführungen entsprechend.[1475]

bb. Technische Schutzmaßnahmen

Auch im Folgenden interessieren die Pflichten eines VPN-Auftraggebers zur Sicherstellung technischer Schutzmaßnahmen, und zwar im Hinblick auf den Unternehmensserver.[1476]

aaa. Verschlüsselung

Verschlüsselungsmaßnahmen gehören zu den Pflichten, die seitens eines Diensteanbieters im Sinne von § 3 Nr. 6 TKG als technische Schutzmaßnahmen gemäß § 109 TKG zu erfüllen sind.[1477]

Vorab soll nochmals auf die gerade dargestellten unterschiedlichen Funktionen und Dienste Bezug genommen werden, die ein VPN zur Verfügung stellen kann: Zum einen finden die Regelungen der §§ 91 ff. TKG im Hinblick auf die Protokollierung der Logdateien Anwendung, sofern der Nutzer die Möglichkeit erhält „für eigene Zwecke“ Daten auf den Server des VPN-Auftraggebers zu übertragen. Zum anderen finden die datenschutzrechtlichen Regelungen des

[1475] Siehe hierzu S. 177 ff.
[1476] Vgl. das Prüfungsschema auf S. 106 ff., insbesondere S. 110 ff.
[1477] Siehe hierzu S. 111 ff.

BDSG Anwendung, sofern Nutzer und VPN-Auftraggeber identische Zwecke verfolgen und es sich insoweit um eine Kommunikationseinheit handelt.

(1) Telekommunikationsdienst

Eine Pflicht zum Angebot von Verschlüsselungsmaßnahmen ergibt sich für den Anbieter eines Telekommunikationsdienstes gemäß § 109 Abs. 1 TKG, der geschäftsmäßig Telekommunikationsdienste gemäß § 3 Nr. 10 TKG erbringt. Diese Verpflichtung wird relevant, wenn der VPN-Auftraggeber dem Nutzer eine Kommunikationsmöglichkeit zur Datenübertragung zur Verfügung stellt, damit dieser eigene und vom VPN-Auftraggeber unabhängige bzw. externe Zwecke erfüllen kann.[1478] So kann der Nutzer etwa Bestellungen für eigene Zwecke tätigen, oder aber im Wege des Online-Backup-Verfahrens seine Daten auf den Server des VPN-Auftraggebers übertragen.[1479]
Zu berücksichtigen ist aber im Rahmen von § 109 Abs. 1 TKG, dass nur angemessene technische Vorkehrungen notwendig sind.[1480] Die jeweiligen Schutzmaßnahmen sind außerdem von den konkret angebotenen Telekommunikationsdiensten abhängig und es müssen nicht alle erdenklichen technischen Maßnahmen getroffen werden.[1481] Daher ist im Verhältnis zu den Nutzern zu prüfen, ob der Einsatz von IPSec erforderlich ist, insbesondere da die Daten mit Wissen und Willen des Nutzers von ihm selbst übertragen werden. Daher kann im Einzelfall ebenso ausreichen, dass andere Verschlüsselungstechniken, wie etwa SSL,[1482] eingesetzt werden.
Bei der Bereitstellung einer Datenübertragungsmöglichkeit durch den VPN-Auftraggeber, etwa einer Bestellmöglichkeit für den Nutzer, ist insoweit kein Unterschied zu Online-Banking oder Webformularen zu sehen, bei welchem dieses Protokoll zurzeit regelmäßig eingesetzt wird. SSL nimmt sämtliche für die Authentizität. Vertraulichkeit und Unversehrtheit der Daten benötigten

---

[1478] Siehe hierzu S. 341 ff.
[1479] Zum Online-Backup siehe S. 74/82.
[1480] Vgl. auch die Ausführungen im zweiten Abschnitt auf S. 110 ff.
[1481] Vgl. Ehmer in: TKG-Kommentar (2. Auflage), § 87 TKG Rn. 24/29; siehe zur Verhältnismäßigkeit und Angemessenheit des § 109 TKG auch Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 21 ff. Vgl. auch Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 87 TKG(1998), Band 1, Rn. 9.
[1482] Siehe zu SSL oben S. 196.

Aufgaben wahr.[1483] Server, die die SSL-Verschlüsselungsverfahren bereitstellen, sind beim jeweiligen Website-Aufruf im Browser anstatt mit „http" mit „https" (secure Hypertext Transfer Protocol) gekennzeichnet.[1484]
Es ist allerdings fraglich, ob IPSec nicht zukünftig dieses Protokoll als Stand der Technik ablösen wird.[1485] So wird im Rahmen der Bewertung der Sicherheit von SSL teilweise zur Vorsicht angeraten.[1486] SSL ist zwar kein charakteristisches VPN-Tunneling-Protokoll, da es nur für bestimmte Client-Server-Applikationen definiert ist.[1487] Dennoch geht zum einen der Trend zu Gesamtlösungen, so dass es zu einer Koexistenz eines VPN mit anderen Sicherheitsprotokollen kommen kann.[1488] Zum anderen kann sich auch im Rahmen eines „klassischen" VPN die Frage stellen, ob starke Verschlüsselungen wie IPSec unbedingt notwendig sind, oder im Einzelfall beispielsweise geringere Verschlüsselungen, wie PPTP, ausreichen könnten.[1489] Denn in diesen Fällen wäre unter Berücksichtigung des spezifischen Telekommunikationsdienstes eine angemessene Schutzmaßnahme getroffen und erfüllt.[1490]
Zwar wird beim Sachverhalt des Ausfüllens eines Webformulars und Online-Banking vertreten, dass die Regelungen des TDDSG und des BDSG in Betracht kommen, wobei das BDSG auf die so genannten Inhaltsdaten anwendbar ist.[1491]
Dieser Auffassung ist jedoch lediglich insoweit zu folgen, dass Nutzungsdaten eines Teledienstes unter die Regelungen des TDDSG fallen und Inhaltsdaten entsprechend den Regelungen des BDSG verarbeitet werden müssen, da sich bei letzteren kein Unterschied zu einer Verarbeitung ohne Einsatz des Internets

[1483] Campo/Pohlmann, Virtual Private Networks, S. 202.
[1484] Siehe zu „http" S. 23. Siehe zum Protokoll „https" Abel, Praxishandbuch, IT-Know-how für den Datenschutzbeauftragten, Teil 1/4 (Glossar) sowie Schmitz in: Spindler/Schmitz/Geis, § 4 TDDSG Rn. 34, wobei hier allerdings ein Druckfehler unterlaufen ist, da fälschlicherweise auf das Protokoll http verwiesen wird, was aber gerade kein Sicherheitsprotokoll darstellt.
[1485] Siehe oben Fn. 4 und dem Hinweis auf den Beitrag in der Frankfurter Allgemeinen Zeitung vom 23.08.2004, S. 17, wo darauf verwiesen worden ist, dass Schweizer Banken mit Virtuellen Privaten Netzwerken arbeiten.
[1486] Campo/Pohlmann, Virtual Private Networks, S. 203.
[1487] Siehe Campo/Pohlmann, Virtual Private Networks, S. 203.
[1488] So Campo/Pohlmann, Virtual Private Networks, S. 201.
[1489] Zu PPTP siehe S. 36.
[1490] Vgl. die obigen Ausführungen und den Verweis in Fn. 1481 auf Ehmer in: TKG-Kommentar (2. Auflage), § 87 TKG Rn. 24/29. Vgl. zur Verhältnismäßigkeit und Angemessenheit des § 109 TKG auch Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 21 ff.
[1491] Siehe zu den Inhaltsdaten S. 105. Vgl. außerdem zum Ausfüllen eines Webformulars Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 121 (unter anderem zu den Unterrichtungspflichten).

ergibt.[1492] Aber das TKG und die damit verbundene Pflicht zur Verschlüsselung ist allein für den Telekommunikationsvorgang anwendbar. Dieser umfasst die Möglichkeit des Nutzers, seine (personenbezogenen) Daten auf den Server des Diensteanbieters zu übertragen.[1493] Für die Bereitstellung von inhaltlichen Informationen auf der Website eines Anbieters, ist und bleibt hingegen das TDDSG, und für die Verarbeitung von Inhaltsdaten das BDSG anwendbar.

Entsprechendes muss im Rahmen eines VPN gelten, wenn der VPN-Auftraggeber einem Nutzer für dessen Zwecke eine Bestellmöglichkeit bereitstellt, wobei aber die Verschlüsselungen nicht zwangsläufig die hohen Anforderungen von IPSec erfüllen müssen.
Im Übrigen ist auch bei der Verknüpfung eines VPN mit dem geschäftsmäßigen Bereitstellen eines Online-Backup-Verfahrens, beispielsweise an Tochterunternehmen, zu prüfen, inwieweit welche Verschlüsselungen als angemessen anzusehen sind.[1494] Die Stärke und die Anforderungen an die Verschlüsselung hängen hierbei gleichermaßen von der Verwendung durch das Tochterunternehmen ab. Diesbezüglich muss also darüber hinaus geprüft werden, inwieweit das Tochterunternehmen Daten von Dritten verarbeitet, oder ob lediglich „eigene betriebliche Geheimnisse" im Wege des Online-Backup-Verfahrens verarbeitet werden sollen. Hier zeigt sich wiederum, dass eine Betrachtung sämtlicher beteiligter Interessen eines Online-Dienstes notwendig ist, um die datenschutzrechtlichen Pflichten vollumfänglich prüfen zu können.
§ 109 TKG schützt sowohl die datenschutzrechtlichen als auch datensicherheitsrelevanten Interessen des Nutzers. Hierbei sind aber gleichermaßen die Interessen von weiteren Betroffenen zu berücksichtigen.

[1492] Vgl. die Ausführungen auf S. 105 ff. und den Verweis auf die herrschende Meinung bezüglich der Verarbeitung von Inhaltsdaten (Gola/Müthlein, TDG/TDDSG, § 2 TDG, S. 110; Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2987 Fn. 52; Schaar, Datenschutz im Internet, Rn. 450, 465; Gola/Klug, Grundzüge des Datenschutzrechts, S. 191; Scholz in: Roßnagel, Datenschutz beim Online-Einkauf, S. 44; Schrey/Meister, K&R 2002, 177, 181; Bäumler, DuD 1999, 258, 259; Gola/Müthlein, RDV 1997, 192, 196; Schaar, CR 1996, 170, 172/173). Vgl. zur Anwendbarkeit des BDSG bei der Übermittlung personenbezogener Daten als Inhalt einer E-Mail Däubler, Gläserne Belegschaften?, Rn. 334.

[1493] Zur funktionalen Betrachtungsweise siehe oben S. 66.

[1494] Vgl. auch Ehmer in: TKG-Kommentar (2. Auflage), § 87 TKG Rn. 19 mit der Ausführung, dass die Verpflichtung und Beschränkung auf angemessene technische Schutzvorkehrungen das nach Rechtsstaatsgrundsätzen ohnehin zu beachtende Übermaßverbot betont und verdeutlicht, dass § 87 TKG a.F. restriktiv auszulegen ist. Dies hat sich auch die Neufassung des TKG nicht geändert. Vgl. zur Verhältnismäßigkeit und Angemessenheit des § 109 TKG auch Bock in: TKG-Kommentar (3. Auflage), § 109 TKG Rn. 21 ff.

Inwieweit diesbezüglich eigenständige Pflichten des VPN-Auftraggebers, des Nutzers oder des Providers in Betracht kommen können, wird im vierten Abschnitt dieser Arbeit untersucht.[1495]

Ergänzend ist festzuhalten, dass der Grundsatz des Systemdatenschutzes gemäß § 3a BDSG in § 109 TKG insoweit Berücksichtigung gefunden hat, dass die Verpflichtung zur Sicherheit des Dienstes sich mit dem Systemdatenschutz zur Bildung von Pseudonymen überschneidet, da Verschlüsselung von Daten gleichzeitig die Bildung von Pseudonymen bedeutet.[1496]

(2) Teledienst

Handelt es sich bei dem Abrufverfahren um einen Teledienst gemäß § 2 Abs. 2 Nr. 1 TDG,[1497] dann obliegen dem Diensteanbieter gegenüber dem Nutzer unmittelbar aus dem TDG keine gesetzlich normierten Verpflichtungen, für dessen Datenzugriffe besondere Sicherheitsmaßnahmen bezüglich der Datenübertragung zu treffen, etwa durch das Angebot von Verschlüsselungsverfahren.[1498]
§ 4 Abs. 3 Nr. 3 TDDSG regelt zwar die Verpflichtung des Teledienstanbieters sicherzustellen, dass der Nutzer die Teledienste gegen die Kenntnisnahme Dritter geschützt in Anspruch nehmen kann. So ergibt sich aber aus dieser Regelung keine unmittelbare Verpflichtung zur Verschlüsselung bei der Datenübertragung.[1499] Das Gebot, die Vertraulichkeit der Daten zu schützen, bezieht sich bei Diensten im Internet vielmehr auf den internen Verarbeitungsvorgang.[1500] Der (Internet-)Server muss so gesichert sein, dass Dritte keinen Einblick nehmen können. Würde die Regelung des § 4 Abs. 4 Nr. 3 TDDSG und die dort normierte Verpflichtung zur Verschlüsselung vollumfänglich gelten, so wäre jeder Website-Betreiber angehalten, den Zugriff

[1495] Siehe S. 380 ff.
[1496] Siehe hierzu auch Schaar, Datenschutz im Internet, Rn. 163, der ausführt, dass öffentliche Schlüssel, die vom Nutzer durch Verwendung von geeigneter Software erzeugt werden, zu den selbst erzeugten Pseudonymen gehören.
[1497] Vgl. hierzu die Ausführungen auf S. 310 ff.
[1498] Schmitz in: Spindler/Schmitz/Geis, § 4 TDDSG Rn. 34.
[1499] Schmitz in: Spindler/Schmitz/Geis, § 4 TDDSG Rn. 34.
[1500] Schmitz in: Spindler/Schmitz/Geis, § 4 TDDSG Rn. 34.

auf seine Website lediglich unter der Voraussetzung des verschlüsselten Zugriffs zuzulassen.
Diese Möglichkeit kann aber nur in Betracht kommen, wenn es sich um persönliche bzw. personenbezogene Daten des Nutzers handelt. Sofern man jedoch im Einklang mit der in dieser Arbeit vertretenen Auffassung davon ausgeht, dass es sich bei der Bereitstellung der Übertragungsmöglichkeit um einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG handelt, so folgt die Notwendigkeit der Bereitstellung einer Verschlüsselungsmöglichkeit bereits aus § 109 TKG. Die Regelung des § 4 Abs. 4 Nr. 3 TDDSG kann damit nicht unmittelbar herangezogen werden, um eine Pflicht zur Verschlüsselung der Datenübertragung im Internet zu begründen.[1501]
Bei einem VPN ist die Bereitstellung eines Verschlüsselungsverfahren (im Rahmen eines Teledienstes) **im hier untersuchten Personenverhältnis** „VPN-Auftraggeber/Nutzer" ohnehin nicht von Bedeutung, da es sich vornehmlich um Daten handeln wird, an deren Verschlüsselung der VPN-Auftraggeber ein größeres Interesse hat als der Nutzer. Die Pflicht zur Verschlüsselung dieser bereitgestellten Daten kann sich jedoch im Personenverhältnis „VPN-Auftraggeber/Betroffener" ergeben, was an späterer Stelle untersucht wird.[1502] Daher zeigt sich auch an dieser Stelle die Relevanz der Betrachtung des Mehrpersonenverhältnisses.

bbb. Weitere technische und organisatorische Anforderungen

Da der VPN-Auftraggeber den Server nicht einer Öffentlichkeit zur Verfügung stellt, kommen Maßnahmen gemäß § 109 Abs. 2 TKG nicht in Betracht.
Der VPN-Auftraggeber ist allerdings bei geschäftsmäßigen Handeln verpflichtet, die technischen und organisatorischen Maßnahmen sicherzustellen, die notwendig sind, um unbefugte Kenntnisnahmen bezüglich der Zugriffe durch die Nutzer zu verhindern, und damit das Fernmeldegeheimnis gemäß § 88 Abs. 1 TKG zu wahren.[1503] Diesbezüglich muss im Einzelfall geprüft werden, welche Maßnahmen, neben der oben dargestellten Verschlüsselung, außerdem in Betracht kommen können. Ein wichtiger Punkt stellt in diesem Zusammenhang

[1501] Ebenso Schmitz in: Spindler/Schmitz/Geis, § 4 TDDSG Rn. 34.
[1502] Siehe S. 403 ff., insbesondere S. 412.
[1503] Vgl. Post-Ortmann, RDV 1999, 102, 103.

etwa die organisatorische Maßnahme von gesicherten Räumlichkeiten gemäß § 9 BDSG dar, in welchen der Server untergebracht ist.[1504]

cc. Überwachungsmaßnahmen und Auskunftsersuchen

Anbieter von geschäftsmäßig erbrachten Telekommunikationsdiensten können gemäß § 113 TKG zur Auskunft über verarbeitete Daten oder zur Überwachung[1505] verpflichtet sein. Maßnahmen nach der TKÜV werden allerdings regelmäßig ausscheiden, da der VPN-Auftraggeber kein an die Allgemeinheit gerichtetes Angebot zur Verfügung stellt.[1506]

Durch § 113 Abs. 1 S. 2 TKG ist der VPN-Auftraggeber allerdings zur Auskunft über Daten gemäß §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO verpflichtet, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird, insbesondere können Strafverfolgungsbehörden die Aufhebung der Benutzerkennungen verlangen. Für die Aufhebung der Datenverschlüsselung bzw. Herausgabe des Datenschlüssels ist dagegen eine gesonderte Anordnung, etwa gemäß § 100b Abs. 3 StPO,[1507] erforderlich, was sich ebenso aus § 113 Abs. 1 S. 3 TKG ergibt.[1508]
Dies bedeutet für den VPN-Auftraggeber, dass auch er gegenüber Behörden zu Überwachungsmaßnahmen verpflichtet ist, sofern er Dritten im Sinne von § 3 Nr. 10 TKG Telekommunikationsdienste anbietet, etwa die oben dargestellte Bestellmöglichkeit für Dritte oder das Angebot des Online-Backup-Verfahrens für Tochterunternehmen. Bei erlaubter Privatnutzung würde sich diese Verpflichtung ebenso auf die Mitarbeiter des VPN-Auftraggebers beziehen. Auch sie stellen in diesem Fall Dritte gemäß § 3 Nr. 10 TKG dar.[1509]

[1504] Siehe Heibey in: Roßnagel, Handbuch Datenschutzrecht, 4.5 Rn. 21 ff., zur Zugangskontrolle Rn. 42. Vgl. auch die Ausführungen von Barta, Datenschutz im Krankenhaus, S. 131 ff..
[1505] Zur TKÜV siehe Fn. 46 sowie S. 118 mit dem Hinweis, dass gemäß § 3 Abs. 2 TKÜV die Vorschriften des § 100b Abs. 3 Satz 1 StPO, des § 2 Abs. 1 Satz 3 des G-10-Gesetzes und des §§ 23 a Abs. 8 des Zollfahndungsdienstegesetzes unberührt bleiben und Diensteanbieter daher auf Anordnung Auskunft über die näheren Umstände der Telekommunikation zu erteilen haben.
[1506] Zur Definition des Telekommunikationsdienstes für die Öffentlichkeit siehe S. 116.
[1507] Siehe hierzu auch die Ausführungen in der Einführung S. 13.
[1508] Siehe hierzu auch die obigen Ausführungen auf S. 261 ff. unter Verweis auf Bäumler in: Roßnagel, Handbuch Datenschutzrecht, 8.3 Rn. 57.
[1509] Siehe hierzu S. 320 ff.

Zu berücksichtigen ist hierbei aber, dass Anordnungen in diesem Falle ins Leere laufen können, da sich zum einen der VPN-Auftraggeber nicht selbst belasten darf, und zum anderen ohnehin „vorgewarnt“ wäre.

b. Gateway

Sofern der VPN-Auftraggeber die Funktionsherrschaft über den Gateway innehat,[1510] liegt zwar ein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG vor, aber die §§ 91 ff. TKG finden nur Anwendung, sofern die Diensterbringung geschäftsmäßig (an Dritte) erfolgt. Daher sind die Protokolle, die auf dem Gateway entstehen, und sich auf Zugriffszeiten, etc. beziehen bei geschäftsmäßigem Handeln gemäß § 96 Abs. 2 TKG zu löschen sind, sofern sie nicht für Zwecke der §§ 97, 99 und 100 TKG benötigt werden.[1511] Bei nicht geschäftsmäßigem Handeln sind diese Protokolle dagegen gemäß § 35 Abs. 2 Nr. 3 BDSG zu löschen, sofern sie nicht mehr für die Aufrechterhaltung des Betriebs benötigt werden.[1512] Letzteres kommt insbesondere bei Mitarbeitern in Betracht, kann aber ebenso in Bezug auf Externe oder Tochterunternehmen in Betracht kommen, sofern diese mit der Nutzung des VPN keine eigenen Zwecke verfolgen, sondern insoweit mit dem VPN-Auftraggeber eine Kommunikationseinheit bilden.[1513]

Die auf dem Gateway stattfindende Authentifizierung der Nutzer ist unerlässliche Voraussetzung, um unberechtigte Zugriffe auf das Unternehmensnetz zu vermeiden.[1514] Auch hier ergibt sich die Legitimation der Einrichtung eines Authentifizierungssystems bzw. die Zulässigkeit der Speicherung der Authentifizierungsdaten auf dem Gateway oder Server nicht aus dem TKG oder TDDSG sondern aus dem BDSG, da die (erstmalige) Speicherung und Verknüpfung der jeweiligen Authentifizierungsmerkmale nicht

[1510] Siehe zur Funktionsherrschaft S. 149 ff., dort unter anderem den Verweis auf Bothe/Heun/Lohmann, ArchivPT 1995, 5, 18/20.
[1511] Vgl. hierzu oben S. 341 ff.
[1512] Siehe Schaffland/Wiltfang, BDSG, § 35 BDSG Rn. 33 zum Wegfall der Zweckerfüllung.
[1513] Siehe zur Trennung zwischen eigenen und identischen Zwecken die obigen Ausführungen auf S. 337 ff.
[1514] Siehe zur Funktion eines Gateways oben S. 46 ff.

erst „bei“ der Erbringung eines Telekommunikationsdienstes oder Teledienstes stattfindet, sondern zeitlich früher.[1515]
Zulässigkeitsnorm ist insoweit § 28 Abs. 1 Nr. 2 BDSG, da die Authentifizierung auf den Systemen vorrangig den Interessen des VPN-Auftraggebers und nicht der Zweckbestimmung des Vertragsverhältnisses mit dem Nutzer dient.[1516] Dies gilt sowohl im Hinblick auf ein Arbeitsverhältnis als auch im Hinblick auf Vertragsverhältnisse mit Dritten bzw. Externen, denen der VPN-Auftraggeber Zugriff auf sein Unternehmensnetz gewähren möchte. Der VPN-Auftraggeber hat ein berechtigtes Interesse daran, lediglich legitimierten Personen Zugriff auf sein Unternehmensnetz zu gewähren. Da der Datenverwender hierbei verpflichtet ist, eine Auswahl zu treffen, sich also auf die Daten zu beschränken, ohne deren Verarbeitung sich der jeweilige Vertragszweck nicht erfüllen lässt,[1517] muss er sich, und zwar ebenso aus Gründen des Systemdatenschutzes gemäß § 3a BDSG, solche Authentifizierungssysteme einsetzen, die eine pseudonyme Nutzung ermöglichen. Eine Authentifizierung mittels Namen der Nutzer ist daher zu vermeiden, soweit es andere gleichwertige Authentifizierungsmöglichkeiten gibt.[1518]
Die vorrangige Frage ist daher auch hier, ob es erforderlich ist,[1519] personenbezogene Daten zu speichern bzw. ob eine Authentifizierung mittels Benutzernamen, der aus dem Namen des Nutzers besteht,[1520] datenschutzrechtlich in Betracht kommen kann. Hierbei ist der VPN-Auftraggeber verpflichtet, solche Systeme einzurichten, die eine pseudonyme oder anonyme Nutzung zulassen.[1521]
Eine solche Verpflichtung gehört nicht nur zu den Maßnahmen einer adäquaten Datenvermeidung gemäß § 3a BDSG, sondern stellt darüber hinaus eine Maßnahme dar, die der VPN-Auftraggeber als Diensteanbieter gemäß § 3 Nr. 6 TKG im Sinne von §§ 88, 109 Abs. 1 TKG gegenüber Dritten zu treffen hat, was

[1515] Vgl. hierzu S. 226 ff.
[1516] Vgl. zum eigenen Geschäftszweck S. 208.
[1517] Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 94.
[1518] Zu den Möglichkeiten der Authentifizierung siehe etwa Lipp, VPN, S. 145 ff.
[1519] Siehe zur Erforderlichkeit S. 98.
[1520] Vgl. zu dieser Authentifizierungsmöglichkeit S. 59 ff.
[1521] Vgl. auch Noll/Wedde, Gesetzestexte für die Arbeitswelt, S. 425 mit dem Hinweis, dass seit der Gesetzesnovelle des BDSG Gestaltung und Auswahl von Datenverarbeitungssystemen immer mit dem Ziel der Datenvermeidung und Datensparsamkeit erfolgen muss, und, soweit möglich, eine Anonymisierung und Pseudonymisierung der verwendeten Daten durch den Arbeitgeber vorgenommen werden muss. Die Einhaltung dieser Vorgaben können Betriebs- bzw. Personalräte sowie Beschäftigte einfordern (Noll/Wedde aaO).

dann Auswirkung hat, sofern der Nutzerden Telekommunikationsdienst geschäftsmäßig nutzt. Denn so kann der Umstand, dass Nutzer X bei dem Unternehmen Y beschäftigt oder als Lieferant für dieses Unternehmen tätig ist, ein personenbezogenes Datum bzw. ein Datum darstellen, welches unter das Fernmeldegeheimnis fällt, insbesondere sofern daraus Schlüsse im Hinblick auf das persönliche Nutzungsverhalten des Nutzers gezogen werden können und dieses widerspiegeln. Letzteres ist etwa dann vorstellbar, sofern für einen Dritten nachvollziehbar wäre, dass der bei dem Unternehmen Y angestellte Nutzer X bevorzugt nachts arbeitet, oder erkennbar ist, welchen Beruf der Nutzer ausübt.
Ergänzend ist anzumerken, dass dies bei einem Software-VPN entsprechend gilt, da hier die Authentifizierung der Nutzer auf dem jeweiligen Rechner bzw. Server stattfindet.[1522]

Im Hinblick auf technische Schutzmaßnahmen wurde dargelegt,[1523] dass die unverschlüsselte Datenübertragung vom Gateway ins Unternehmensnetz kritisch sein kann, da eine Telefonleitung grundsätzlich nicht abhörsicher ist. Dementsprechend muss der VPN-Auftraggeber Verschlüsselungstechniken auch „auf diesem letzten Weg“ bereitstellen, die eine entsprechende Sicherheit der Daten zu leisten vermögen, sofern der Gateway geschäftsmäßig bereitgestellt wird.[1524]
Der VPN-Auftraggeber muss daher in diesem Falle, auch wenn es sich bei einem VPN um eine geschlossene Benutzergruppe handelt,[1525] Maßnahmen zum Schutz des Fernmeldegeheimnisses gemäß § 88 TKG und personenbezogenen Daten sowie zur Abwehr von unerlaubten Zugriffen auf den Gateway treffen. Maßnahmen zum Schutz der Infrastruktur, z.B. vor Störungen, äußeren Angriffen und Katastrophen, sowie die Erstellung eines Sicherheitskonzeptes obliegen dagegen nach § 109 Abs. 2, Abs. 3 TKG nur

[1522] Siehe zum Software-VPN S. 53 ff.
[1523] Vgl. Fn. 1101.
[1524] Vgl. hierzu oben S. 341 ff.
[1525] Siehe hierzu S. 335 ff. sowie zur weiteren Definition einer geschlossenen Benutzergruppe S. 184 ff. Siehe aber zur Ablehnung einer geschlossenen Benutzergruppe im Verhältnis zwischen Provider und VPN-Auftraggeber/Nutzer S. 184 ff.

Betreibern öffentlicher Telekommunikationsanlagen, so dass insoweit geschlossene Benutzergruppen privilegiert sind.[1526]

Auch bezüglich der Durchführung von Auskunfts- und Überwachungsmaßnahmen gilt die zum Firmenserver entwickelte Lösung entsprechend, so dass entsprechende vom VPN-Auftraggeber durchzuführende Maßnahmen grundsätzlich nur bei geschäftsmäßigem Handeln nach § 113 Abs. 1 TKG oder Anordnungen, etwa nach §§ 100a, 100b Abs. 3 StPO, in Betracht kommen können.[1527] Hier muss ebenso berücksichtigt werden, dass der VPN-Auftraggeber sich nicht selbst belasten muss.

c. Zwischenergebnis

Der VPN-Auftraggeber darf die Zugriffsdaten der Nutzer umfassend protokollieren, sofern weder geschäftsmäßiges Handeln noch ein öffentliches Angebot-Nutzer-Verhältnis in Betracht kommt.
Hieran ist aber stets die Notwendigkeit zu messen bzw. die Frage zu stellen, inwieweit diese Protokollierung für das Arbeitsverhältnis oder für die Aufrechterhaltung des ordnungsgemäßen Betriebs gemäß § 28 Abs. 1 Nr. 1 BDSG im Sinne eines „Müssens" erforderlich ist.
Ist beispielsweise noch ein Gateway „zwischengeschaltet", dessen Funktion auch darin besteht, nur legitimierten Nutzern Zugriff auf das Unternehmensnetz zu gewähren,[1528] dann muss geprüft werden, inwieweit darüber hinaus auf dem Unternehmensserver eine Notwendigkeit besteht, die Nutzerzugriffe zusätzlich zu protokollieren. Missbräuchliche Nutzung wird insoweit bereits durch den Gateway verhindert.

Der VPN-Auftraggeber muss die Protokolldaten darüber hinaus gemäß § 35 Abs. 2 Nr. 3 BDSG löschen, sofern er diese nicht mehr für Zwecke der Aufrechterhaltung eines ordnungsgemäßen Betriebs benötigt. Daraus ergibt sich, dass ein VPN-Auftraggeber auf seinen Betrieb bezogen prüfen muss, für

[1526] Siehe bereits die Ausführungen in der Einführung S. 112 ff. sowie Zimmer, CR 2003, 893, 896. Vgl. außerdem den Hinweis auf den IT-Grundschutz-Katalog (Fn. 496).
[1527] Siehe hierzu oben S. 351.
[1528] Siehe zur Funktion eines Gateway S. 46 ff.

welchen Zeitraum die Aufbewahrung von Protokollen grundsätzlich notwendig ist

Stellt der VPN-Auftraggeber externen Nutzer den Unternehmensserver ebenso in dem Sinne geschäftsmäßig gemäß § 3 Nr. 10 TKG in Verbindung mit § 91 TKG zur Verfügung, dass diese eigenständig Daten dorthin übertragen oder speichern können, so muss er erstellte Protokolle unverzüglich nach Ende der jeweiligen Verbindung gemäß § 96 Abs. 2 TKG löschen, sofern nicht die Zwecke der §§ 97, 99 und 100 TKG eine längerfristige Speicherung rechtfertigen. Dies gilt ebenso bei einer erlaubten Privatnutzung durch Arbeitnehmer.
Dies bedeutet, dass der VPN-Auftraggeber insoweit getrennte Systeme einsetzen müsste, sofern er im Hinblick auf seine ausschließlich dienstlich agierenden Mitarbeiter eine umfassende Protokollierung anstrebt.[1529] Denn aus § 3 Nr. 6 TKG ergibt sich, dass es ebenso möglich ist, dass ein Diensteanbieter dennoch den Verpflichtungen des §§ 88, 91 ff. TKG unterliegt, auch wenn er Telekommunikationsdienste nur teilweise geschäftsmäßig erbringt. Daher empfiehlt sich der getrennte Betrieb, da ihn anderenfalls die datenschutzrechtlichen Verpflichtungen vollumfänglich treffen würden, zumindest im Hinblick auf den Datentransport.
Im Rahmen der datenschutzrechtlichen Pflichten bei der VPN-Kommunikation ist dementsprechend danach zu unterscheiden, ob es sich um eine Kommunikationseinheit handelt, oder ob der jeweilige Nutzer eigene Zwecke verfolgt. Konsequenz ist, dass beim Zugriff auf den Server der Firmenzentrale kein Datenschutzrecht im Sinne des TKG oder TDDSG Anwendung findet, sofern VPN-Auftraggeber und Nutzer identische Zwecke verfolgen. Die datenschutzrechtlichen Regelungen der §§ 91 ff. TKG finden jedoch Anwendung, sofern der Nutzer eigene Zwecke verfolgt.

[1529] Vgl. auch Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 27, der in seinen Ausführungen darlegt, dass das Fernmeldgeheimnis ebenso auf die geschäftliche Kommunikation ausstrahlen kann, sofern keine Trennung zwischen geschäftlicher und privater Kommunikation auf den Telekommunikationsanlagen möglich ist.

3. Zusatzdienst E-Mail

Entsprechend der Aufbaulogik dieser Arbeit werden im Folgenden die datenschutzrechtlichen Pflichten (Datenvermeidung, Technische Schutzmaßnahmen und Auskunfts- und Überwachungsmaßnahmen) des Zusatzdienstes E-Mail geprüft.[1530] Hierbei wird eine Unterteilung der Nutzer in Mitarbeiter und Kommunikationspartner des VPN-Auftraggebers vorgenommen.[1531] Im Hinblick auf die Mitarbeiter wird außerdem danach unterschieden, inwieweit der zur Verfügung gestellte E-Mail-Account dienstlich oder privat genutzt wird.

a. Mitarbeiter

Die nachfolgenden Ausführungen beziehen sich auf die datenschutzgerechte Verarbeitung der Daten der Mitarbeiter des VPN-Auftraggebers.

aa. Datenvermeidung

Im Sinne optimalen Datenvermeidung steht auch hier die Frage im Mittelpunkt, welche Mitarbeiterdaten im Einzelfall anfallen und gelöscht werden müssen.[1532]

aaa. Dienstliche Nutzung

Bezüglich der dienstlichen Nutzung gelten die Ausführungen zum zwangsweisen Tunneling entsprechend.[1533] Ist seitens des Arbeitgebers lediglich die dienstliche Nutzung des E-Mail-Accounts erlaubt und die private Nutzung explizit verboten, so darf er die anfallenden Daten der E-Mail-Kommunikation ebenso wie deren Inhalt umfassend gemäß § 28 Abs. 1 Nr. 1 BDSG protokollieren und entsprechende Log-Files erstellen.[1534] Dies gilt aber

[1530] Vgl. S. 106 ff. zu den datenschutzrechtlichen Pflichten sowie S. 162 ff., 280 ff. zum bisherigen Aufbau der Arbeit, der im jeweiligen Personenverhältnis in einem zweiten Teil stets die datenschutzrechtliche Prüfung erfasst.
[1531] Vgl. S. 83, 279, 302.
[1532] Vgl. S. 106 ff.
[1533] Siehe oben S. 320 ff.
[1534] Siehe zu Log-Files S. 178. Siehe auch Kramer, NZA 2004, 457, 460 zur Verletzung der arbeitsvertraglichen Pflichten durch den Arbeitnehmer, sofern keine Regelung über eine private

lediglich unter der Voraussetzung, dass die Protokollierung für die Sicherstellung des ordnungsgemäßen Betriebs erforderlich ist, da diese der Zweckbestimmung des Arbeitsverhältnisses dient.[1535]
Auch hier müssen entsprechende nachvollziehbare Regelzeiten entwickelt werden, in welchen die Löschung der Daten erfolgt, und es darf ebenso wenig in diesem Zusammenhang durch „die Hintertür“ das Verhalten der Mitarbeiter kontrolliert werden.[1536] Es müssen tatsächlich technische Erfordernisse die Protokollierung erforderlich machen. Eine weitergehende Protokollierung kann nur mit Einwilligung des Arbeitnehmers oder durch Wahrnehmung der Mitbestimmung des Betriebsrates erfolgen, wobei der Betriebsvereinbarungen den Schranken des § 75 Abs. 2 BetrVG unterliegen.[1537]

Im Hinblick auf die Verhaltens- und Leistungskontrolle kann eine Protokollierung daher nur gemäß § 28 Abs. 1 Nr. 2 BDSG in Betracht kommen. Dies muss aber regelmäßig ausscheiden, sofern nicht ausnahmsweise ein berechtigtes Interesse des VPN-Auftraggebers bzw. Arbeitgebers vorliegt und das Interesse des Arbeitnehmers nicht überwiegt.[1538] Starre Vorgaben sind in diesem Zusammenhang schwierig. Sofern aber tatsächliche und konkrete Anhaltspunkte dafür vorliegen, dass der Betriebsablauf aufgrund übermäßiger Internetnutzung tatsächlich zum Stillstand kommt, kann darin möglicherweise (und ausnahmsweise) ein berechtigtes Interesse des VPN-Auftraggebers bzw. Arbeitgebers liegen. In diesem Falle kann sich eine Verhaltenskontrolle (bei konkretem Verdacht) aber nur darauf beziehen, ob der E-Mail-Dienst unberechtigterweise privat genutzt worden ist, wobei die Beteiligungsrechte des

Internetnutzung im Betrieb existiert. Vgl. außerdem zur unerlaubten Privatnutzung Däubler in: Ahrens/Donner/Simon, Arbeit-Umwelt, 2001, S. 1, 6/7. Vgl. zur arbeitsrechtlichen Konsequenz der „klarstellenden“ Ermahnung, wenn für den Arbeitnehmer unklar war, dass die private Nutzung ausgeschlossen ist, Däubler, K&R 2000, S. 323, 327.

[1535] Siehe zur Erforderlichkeit auch S. 98.

[1536] Siehe hierzu S. 324 ff./ 328 ff.

[1537] Vgl. Wedde, DuD 2004, 169, 174. Siehe außerdem Matthes in: Münchener Handbuch Arbeitsrecht, § 338 Rn. 51 mit dem Hinweis, dass im Rahmen von Betriebsvereinbarungen zu technischen Überwachungsmaßnahmen die nähere Ausgestaltung der Regelung der Einigung durch die Betriebspartner unterliegt. Daher sind einer solchen Betriebsvereinbarung grundsätzlich auch Regelungen zu Löschungsfristen denkbar. Vgl. zur Mitbestimmung des Betriebsrates im Rahmen von Protokollierungen auch Leopold, DuD 2006, S. 274, 276.

[1538] Vgl. auch Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 79; Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 27/31 ff. A.A. Raffler/Hellich, NZA 1997, 862, 867, die ein Recht des Arbeitgebers zur Kontrolle der E-Mail-Nutzung der Arbeitnehmer für den Fall annehmen, dass diese Kontrolle der Feststellung dient, ob die E-Mail-Nutzung nur betrieblichen Zwecken dient und nicht für private oder gar rechtswidrige Zwecke missbraucht wird.

Betriebsrates zu beachten sind.[1539] Existiert kein Betriebsrat, müssen die Anforderungen an die berechtigten Interessen des Arbeitgebers noch höher angesetzt werden. Hier können eine Protokollierung oder gar Einsichtsrechte in die E-Mails allenfalls bei begründetem Verdacht strafbarer Handlungen in Betracht kommen.[1540]

Es besteht im Übrigen eine Parallele zum Telefonverkehr. Die Erfassung der Begleitumstände (Beginn und Ende, vertelefonierte Einheiten, angerufene Nummer) ist dort ebenfalls grundsätzlich zulässig.[1541] Dennoch muss insgesamt unterschieden werden, ob die Aufzeichnung für die Sicherstellung des ordnungsgemäßen Betriebs erforderlich ist. In diesem Fall können auch kurze Löschungsfristen von zwei Wochen in Betracht kommen.[1542] Die generelle und durchgängige Überwachung von Mitarbeitern ist allerdings nicht gemäß § 28 Abs. 1 Nr. 1 BDSG im Sinne eines Muss erforderlich und würde ebenso der Vorgabe des § 3a BDSG widersprechen. Daher ist gemäß § 28 Abs. 1 Nr. 2 BDSG abzuwägen, ob der Betriebsablauf aufgrund tatsächlicher Anhaltspunkte tatsächlich gestört ist.
Dies steht im Einklang mit der gesetzlichen Intention von § 28 BDSG. Zum einen sind bei der Datenerhebung nach § 28 Abs. 1 S. 2 BDSG die Zwecke vom Arbeitgeber konkret festzulegen.[1543] Zum anderen dürfen für die bestimmte Zwecke erhobenen Daten gemäß § 28 Abs. 2 BDSG für andere Zwecke nur dann genutzt werden, wenn die Voraussetzungen des § 28 Abs. 1 Nr. 2 und Nr. 3 BDSG vorliegen.[1544]

Bei der Sicherstellung des ordnungsgemäßen Betriebs kommt zudem (anders als bei der reinen Protokollierung von Zugriffsdaten im Rahmen der Internetnutzung) noch ein weiterer Aspekt hinzu, der sich auf die Löschungsfristen auswirkt. Der Arbeitgeber ist naturgemäß daran interessiert, die E-Mail-Daten (insbesondere deren Inhalt) längerfristig zu speichern. Das

[1539] Vgl. Däubler, K&R 2000, 323, 327.
[1540] Vgl. Däubler aaO. Siehe zu den Beteiligungsrechten des Betriebsrats die obigen Ausführungen auf S. 328 ff. Vgl. in diesem Zusammenhang auch die nachfolgenden Ausführungen zur privaten E-Mail-Nutzung auf S. 362 ff.
[1541] Vgl. Däubler in: Ahrens/Donner/Simon, Arbeit-Umwelt, 2001, S. 1, 4; Post-Ortmann, RDV 1999, 102, 106/107; Ernst, NZA 2002, 585, 589 ff.
[1542] Siehe hierzu S. 180 und S. 324.
[1543] Vgl. auch Däubler, NZA 2001, 874, 876.
[1544] Vgl. auch Däubler, NZA 2001, 874, 877.

Interesse besteht zumindest für die Dauer der Geschäftsbeziehung mit dem E-Mail-Partner bzw. Geschäftspartner. Daher ist orientiert sich die Löschungsfrist gemäß § 35 Abs. 2 BDSG im Hinblick auf erstellte Log-Files und Inhalt vorrangig an der Fragestellung, für welche Dauer der VPN-Auftraggeber bzw. Arbeitgeber ein Interesse an der Aufbewahrung hat. Dies kann aber stets nur im Einzelfall entschieden werden. Ein Vergleich mit dem Telefonverkehr zeigt, dass es allein in der Hand des Mitarbeiters liegt, sich über den Inhalt der Kommunikation entsprechende Notizen zu machen. Sofern er diese unterlässt sind die Informationen verloren, insbesondere wenn der Mitarbeiter aus dem Betrieb ausscheidet. Daher könnte auch hier argumentiert werden, dass der Arbeitgeber aufgrund der Aufrechterhaltung und Sicherstellung des ordnungsgemäßen Betriebs ein Interesse an der Aufzeichnung der Gespräche hat.

Der Lösungsansatz muss allerdings ein anderer sein. Der Mitarbeiter ist während seines Angestelltenverhältnisses dazu angehalten, sämtliche betriebliche Kommunikation unter Berücksichtigung seiner arbeitsvertraglichen Pflichten ordnungsgemäß zu bearbeiten. Dazu gehören sowohl Aktennotizen über wichtige Gespräche als auch das Abheften der E-Mail-Kommunikation oder zumindest deren Verschieben und Speichern in elektronischen Ordnern, die den relevanten Mitarbeitern zur Verfügung stehen.

Der Arbeitgeber muss seine Mitarbeiter bei Bedarf zur Erfüllung dieser Pflichten ggf. nochmals deutlich anweisen.[1545] Er darf aber die Kommunikation nicht mit der Begründung kontrollieren, dass die langfristige Aufbewahrung der E-Mail-Kommunikation der Aufrechterhaltung des Betriebs dient. Daher muss auch hier gelten, dass die Aufzeichnung der Log-Files nur zur Kontrolle des ordnungsgemäßen Ablaufs der technischen Systeme notwendig ist und der Inhalt nicht aufgezeichnet werden darf.

Daher darf der Arbeitgeber den Inhalt E-Mail ohne Einwilligung des Arbeitnehmers nicht speichern und jegliche Einsichtsrechte sind ausgeschlossen. Unverständlich ist die Auffassung, die einerseits zwar darauf verweist, dass E-Mails ähnlich wie Telefonate wenig formell ausgestaltet seien

[1545] Siehe aber auch Schaub, Arbeitsrechts-Handbuch, § 53 Rn. 14 zur Nebenpflicht des Arbeitnehmers, Schäden vom Arbeitgeber als Inhaber des Betriebs abzuwenden (so dass vertretbar erscheint, auch eine ordentliche Dokumentation über wichtige geschäftliche Vorgänge von einer solchen Nebenpflicht zu erfassen). Vgl. zur persönlichen und fachlichen Weisungsgebundenheit eines Arbeitnehmers außerdem Wedde, Telearbeit, S. 23 ff.

und daher über die Persönlichkeit des Einzelnen mehr aussagen können als im Rahmen des herkömmlichen Schriftverkehrs. Andererseits wird aber ohne Begründung verneint, dass damit eine Gleichbehandlung zum Telefonverkehr gerechtfertigt sei.[1546] Richtigerweise ist hier der Persönlichkeitsschutz des Arbeitnehmers gemäß Artikel 2 Abs. 1 GG betroffen und eine Gleichbehandlung zum Recht am gesprochenen Wort gerechtfertigt.[1547] Da auch ein Arbeitgeber (mittelbar) an die Grundrechte gebunden ist,[1548] muss der Arbeitnehmer ebenso bei dienstlichen E-Mails gemäß § 4a BDSG ausdrücklich in die Kenntnisnahme oder etwaige Archivierung der E-Mails einwilligen.
Ausschließlich in diesen Fällen kann die geforderte Pflicht zur Entschlüsselung greifen. [1549]

Im Rahmen der E-Mail-Nutzung gilt daher die Besonderheit, dass zwar einerseits die datenschutzrechtlichen Regelungen des TKG nicht greifen, nach denen der Arbeitgeber gemäß § 88 TKG an das Fernmeldegeheimnis gebunden wäre.[1550] Andererseits ist der Arbeitgeber jedoch (mittelbar) an die Grundrechte gebunden, so dass unter diesem Gesichtspunkt jegliche Einsichtnahme in den Inhalt der Kommunikation ausgeschlossen ist..

[1546] Siehe auch Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 268/269, der darauf verweist, dass anders als bei dienstlichen Telefonaten, der Arbeitgeber bei E-Mails grundsätzlich das Recht hat, vom Inhalt der Korrespondenz Kenntnis zu nehmen.
[1547] Siehe zum Recht am gesprochenen Wort als allgemeines Persönlichkeitsrecht BAG (vom 29.06.2004) AuR 2005, 453, 454, ebenso Wedde, AuR 2005, 453, 457.Siehe außerdem Naujoks, DuD 2002, S. 592, 593, die im Mitlesen bzw. in der Kenntnisnahme des E-Mail-Inhaltes einen nicht zu rechtfertigenden Eingriff in das Persönlichkeitsrecht des Arbeitnehmers sieht. Ebenso Lehnhardt, DuD 2003, S. 487, 488/489, der zwar bei ausschließlich dienstlicher Nutzung Löschungsrechte des Arbeitgebers im Hinblick auf virenbehaftete E-Mails bejaht. Aber bei Einsichtnahme in die E-Mails sieht er auch bei ausschließlich dienstlicher Nutzung aufgrund der Nähe zum gesprochenen Wort einen Eingriff in das allgemeine Persönlichkeitsrecht gegeben. In diesem Sinne ebenso Bijok/Class, RDV 2001, S. 52, 54. Däubler, Internet und Arbeitsrecht, Rn. 249; Däubler, Gläserne Belegschaften?, Rn. 351; Däubler, K&R 2000, S. 323, 326/327. Siehe aber auch Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 46, der dies ablehnt.
[1548] Siehe zur mittelbaren Drittwirkung der Grundrechte im Privatrecht Pieroth/Schlink, Grundrechte, Rn. 173 ff. insbesondere Rn. 181; Siehe zur mittelbaren Drittwirkung der Grundrechte im Arbeitsverhältnis Oetker, RdA 2004, 8, 11; Jarass, NJW 1989, 857, 862.
[1549] Siehe auch Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 274.
[1550] Vgl. auch Däubler, K&R 2000, S. 323, 327.

bbb. Private Nutzung

Der private E-Mail-Verkehr hingegen unterliegt dem Fernmeldegeheimnis, so dass dessen Inhalt nicht gespeichert bzw. in diesen noch nicht einmal Einblick genommen werden darf.[1551]

Da es sich hier nicht um dienstliche Kommunikation handelt, bilden Mitarbeiter und Arbeitgeber bzw. VPN-Auftraggeber keine Kommunikationseinheit, so dass es sich bei dem Mitarbeiter um einen Dritten gemäß § 3 Nr. 10 TKG handelt.[1552] Verbindungsdaten wie Zieladresse, Datum, Uhrzeit, verwendetes Protokoll, etc. sind unmittelbar nach Verbindungsende zu löschen, es sei denn sie würden etwa noch für Abrechnungszwecke benötigt oder es wäre ein konkreter Missbrauchsverdacht gegeben (§ 96 Abs. 2 TKG i.V.m. § 100 Abs. 3 TKG).[1553]

Nach anderer Ansicht soll der Arbeitgeber zur Kontrolle der privaten Nutzung des E-Mail-Kommunikationssystems berechtigt sein, die Verbindungsdaten, mithin Datum und Uhrzeit der Versendung, Datum und Uhrzeit des Empfangs, Größe der Datei sowie verkürzte Adresse des Empfängers erfassen dürfen.[1554] Dies soll insbesondere erlaubt sein, damit der Arbeitgeber die Möglichkeit hat zu prüfen, inwieweit sich seine Mitarbeiter vertragstreu verhalten.[1555]

Dieser Auffassung ist jedoch zu entgegnen, dass der Arbeitgeber noch nicht einmal im Rahmen der dienstlichen Protokollierung diese Daten zur Verhaltens- und Leistungskontrolle nutzen darf bzw. erst dann darauf zurückgreifen darf, sofern sich ein konkreter Missbrauchsverdacht ergibt.[1556] Wenn nun der Arbeitgeber aufgrund eines überwiegenden betrieblichen Interesses nach der hier zitierten Auffassung berechtigt sein soll, die Verbindungsdaten und den E-

[1551] Vgl. oben Fn. 1374 und die dortigen Hinweise auf Siehe etwa Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 79; Gola/Schomerus, BDSG, § 28 BDSG Rn. 20; Gola/Klug, Grundzüge des Datenschutzrechts, S. 198; Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 40 ff., S. 75; Gola, MMR 1999, 322, 325; Hilber/Frik, RdA 2002, 89, 92 ff. (insbesondere S. 94); Mengel, BB 2004, 2014, 2019.

[1552] Siehe hierzu die Ausführungen auf S. 331 sowie S. 339.

[1553] Siehe auch Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 80 ff., insbesondere Rn. 82.

[1554] Ueckert, ITRB 2003, 158, 160; vgl. auch Ernst, NZA 2002, 585, 590.

[1555] Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S.65. Siehe auch Däubler, CR 1994, 754, 759, der bezüglich des Fernsprechgeheimnisses des Arbeitnehmers die Auffassung vertritt, dass es etwas widersprüchlich erscheint, Privatgespräche zu gestatten und sich gleichwohl Kontrollrechte vorzubehalten. Siehe außerdem Hilger, DB 1986, 910, 913;

[1556] Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 79. Zur Strafbarkeit der E-Mail-Kontrolle durch den Arbeitgeber siehe Barton, CR 2003, 839 ff. Siehe zu dieser Thematik ebenso die Ausführungen auf S. 321 ff. Vgl. Ebenso Däubler, K&R 2000. 323, 327.

Mail-Kopf einzusehen,[1557] bedeutet dies im Umkehrschluss ebenso eine umfassende Leistungs- und Verhaltenskontrolle.[1558] Zu berücksichtigen ist hierbei nämlich auch, dass der E-Mail-Kopf vielfach den vollständigen Namen einer Person und vebenso den Namen des Unternehmens enthält, für welches der Inhaber der E-Mail-Adresse arbeitet.[1559]

Außerdem liegt hier ein grundsätzlich anderer Sachverhalt als im Rahmen der Briefpost vor. Hierzu wird richtigerweise vertreten, dass der Arbeitgeber bei einen an das Unternehmen adressierten Brief, der als Empfänger den Namen des Mitarbeiters enthält, diesen öffnen und lesen darf.[1560] Bei einer E-Mail ist allerdings zu beachten, dass diese „privater" ist, als ein offiziell an ein Unternehmen adressierter Brief, bei dem der Versender damit rechnen muss, dass dieser vom Sekretariat geöffnet wird.[1561]

Gleichermaßen ist bei einer E-Mail, die der Mitarbeiter versendet, nicht von vorneherein ersichtlich, ob diese E-Mail (auch) privater oder ausschließlich beruflicher Natur ist.

Zwar wird darauf verwiesen, dass keine Bedenken dagegen bestehen, die privaten Daten des Arbeitnehmers aufgrund einer Einwilligungserklärung umfassend zu protokollieren.[1562] Hiergegen muss jedoch eingewendet werden, dass Zweifel an der Freiwilligkeit einer solchen Einwilligungserklärung bestehen,[1563] da regelmäßig von einem faktischen Druck des Arbeitgebers im

[1557] Vgl. hierzu Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 64, die ihre Auffassung an die Zielnummernerfassung bei privaten Telefongesprächen anlehnen (siehe hierzu auch Schulin/Babel, NZA 1986, 46, 49; Däubler, CR 1994, 754, 759 sowie im Besonderen BAG (27.05.1986), AP Nr. 15, Bl. 7 zu § 87 BetrVG (Überwachung)) und ebenso darauf hinweisen, dass aus diesen äußeren Verbindungsdaten konkrete Rückschlüsse gezogen werden können, beispielsweise wer mit wem kommuniziert, wie lange und welche Datenmengen dabei bewegt werden.

[1558] Zur Kontrollmöglichkeit des Arbeitgebers bezüglich des E-Mail-Verkehrs seiner Nutzer siehe etwa Kleine-Voßbeck, Electronic Mail und Verfassungsrecht, S. 131 unter Hinweis darauf, dass sich im Bereich der E-Mail-Kommunikation weitergehende Kontrollmöglichkeiten als im Bereich der Kommunikation per Telefon ergeben. So könnten beispielsweise auch Verhaltensaspekte eine Rolle spielen, wie etwa die Reaktionszeit eines Arbeitnehmers zur Beantwortung einer E-Mail und die quantitative Ausführlichkeit seiner jeweiligen Antwort. Darüber hinaus dürfte aber auch die Qualität der Antwort eine große Rolle spielen. Tinnefeld, DuD 2002, 231, 235 verweist darauf, dass das Arbeitsverhalten des Nutzers dann lückenlos kontrolliert werden kann, sofern er seine gesamte Arbeit über den vernetzten PC abwickelt. Zu den datenschutzrechtlichen Vorgaben für den Arbeitgeber siehe Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 46 ff. (für den E-Mail-Verkehr siehe S. 53 ff.); Ueckert, ITRB 2003, 158 ff.

[1559] Mengel, BB 2004, 2014, 2016.

[1560] Ernst, NZA 2002, 585, 588; Mengel, BB 2004, 2014, 2016.

[1561] Vgl. Ernst, NZA 2002, 585, 590.

[1562] Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 82.

[1563] Siehe hierzu die Ausführungen im zweiten Abschnitt dieser Arbeit S. 95. Zum Erfordernis der Freiwilligkeit der Entscheidung siehe Holznagel/Sonntag in: Roßnagel, Handbuch Datenschutzrecht, 4.8 Rn. 54. Siehe außerdem Scholz in: Roßnagel, Datenschutz beim Online-

Verhältnis zum Arbeitnehmer ausgegangen werden muss. Es wird sich voraussichtlich kein Arbeitnehmer widersetzen, sofern sein Vorgesetzter von ihm verlangt, in die (Verhaltens-)Kontrolle seiner privaten Internetnutzung einzuwilligen.[1564]

Demgemäß können grundsätzlich Kontrollrechte des Arbeitgebers zwar in Betracht kommen, wobei aber stets für den Einzelfall geprüft werden muss, inwieweit der Arbeitnehmer sich dem Druck des Arbeitgebers gebeugt hat, eine solche Einwilligung abzugeben.[1565] Hierbei ist zu beachten, inwiefern dem Arbeitnehmer vom Arbeitgeber bei Vertragsschluss glaubhaft echte Wahlmöglichkeiten eingeräumt werden.[1566] Ansonsten sind die Daten gemäß § 96 Abs. 2 TKG unverzüglich nach Verbindungsende zu löschen, wobei die Nachweispflicht, dass die getroffene Regelung erforderlich und verhältnismäßig ist, dem Arbeitgeber obliegt. Denn dieser will Rechte aus ihr herleiten und beruft sich auf die Einwilligung.[1567] In diesem Kontext gilt ebenfalls , dass eine Betriebsvereinbarung nicht ohne weiteres die Einwilligung des Arbeitnehmers aufgrund der in § 75 Abs. 2 BetrVG geregelten Persönlichkeitsrechte ersetzen kann.[1568]

Einkauf, S. 51, der darauf verweist, dass der Betroffene tatsächlich ein Wahlrecht zwischen Einverständnis und Verweigerung haben muss und nicht latent einem (auf den ansonsten drohenden Nachteilen beruhenden) Zwang zur Einwilligung ausgesetzt sein darf. Siehe zur Freiwilligkeit der Einwilligung Wedde, DuD 2004, 169, 172. Siehe außerdem Gola/Schomerus, BDSG, § 4a BDSG Rn. 6 mit dem Hinweis, dass die Einwilligung ohne Zwang erfolgen muss. Vgl. außerdem Anmerkung Linnenkohl/Schütz zu BAG, RDV 1987, 129, 134 (noch zu § 3 BDSG a.F.) mit dem Hinweis, dass der Eingriff in das Persönlichkeitsrecht verlangt, dass entweder eine Einwilligung oder die gesetzlichen Erlaubnistatbestände (als allgemeine Zulässigkeitsvoraussetzungen für die Verarbeitung der personenbezogenen Daten) vorliegen müssen. Siehe außerdem Däubler, NZA 2001, 874, 876 mit dem Hinweis, dass eine Einwilligung nur dann rechtfertigende Wirkung entfalten kann, wenn sie „auf der freien Entscheidung" des Betroffenen beruht. Vgl. Wiese, RdA 1986, 120, 127 zur Nichtigkeit der Einwilligung (im Arbeitsverhältnis) gemäß § 138 BGB bei fehlender Freiwilligkeit.

[1564] So Schlachter in: Noack/Spindler, Unternehmensrecht und Internet, S. 216 im Zusammenhang mit einer Einwilligungserklärung des Arbeitnehmers im Rahmen der Telearbeit, die jedoch später in dieser Arbeit (siehe S. 417 ff.) unter einem anderem Gesichtspunkt behandelt wird. Siehe zur Einwilligung „unter Druck" insbesondere auch Däubler, Internet und Arbeitsrecht, Rn. 332a.

[1565] Wedde, DuD 2004, 169, 171 ff. Siehe auch Tinnefeld, MMR 2001, 797, 798, die ausführt, dass der inhaltliche Schutz von privaten oder geschäftlichen E-Mails wegen des grundrechtlichen Schutzes des TK-Geheimnisses nur in Ausnahmefällen in Betracht kommen kann (beispielsweise bei begründetem Verdacht einer strafbaren Handlung).

[1566] Wedde, DuD 2004, 169, 172 ff.

[1567] Wedde, DuD 2004, 169, 172 ff.

[1568] Siehe hierzu bereits die obigen Ausführungen auf S. 328 und 358 sowie Wedde, DuD 2004, 169, 174.

bb. Technische Schutzmaßnahmen

Bei den technischen Schutzmaßnahmen ist zwischen der dienstlichen und der (auch) privaten Nutzung zu trennen.
Im Rahmen der dienstlichen Nutzung erbringt der VPN-Auftraggeber keinen Telekommunikationsdienst an Dritte gemäß § 3 Nr. 10 TKG, so dass er nicht zu Maßnahmen gemäß § 109 Abs. 1 TKG unter Berücksichtigung des Artikels 4 der EU-Richtlinie 2002/58/EG verpflichtet ist. Er wird gegebenenfalls aber im Eigeninteresse darauf hinwirken, dass dienstliche E-Mails lediglich verschlüsselt versendet werden, und zwar unter Berücksichtigung seiner Verpflichtungen gegenüber Betroffenen.[1569]

In Bezug auf die Mitarbeiter, denen er den Dienst ebenso zur privaten Nutzung zur Verfügung stellt, obliegen ihm allerdings die technischen Schutzmaßnahmen gemäß § 109 Abs. 1 TKG, da geschäftsmäßiges Handeln gemäß § 3 Nr. 10 TKG vorliegt.[1570] Aber da der VPN-Auftraggeber diese Verschlüsselung nicht für den Nutzer vornehmen kann, liegt es auch hier in der Verantwortung des jeweiligen Nutzers, seine E-Mails eigenständig zu verschlüsseln.[1571]
Dem VPN-Auftraggeber ist hingegen möglich, gemäß
§ 93 TKG über Verschlüsselungsmöglichkeiten- und techniken zu informieren, so dass bei auch privater Nutzung der E-Mail-Accounts durch die Nutzer bzw. Mitarbeiter eine Information seitens des VPN-Auftraggebers über die gängigen Verschlüsselungstechniken wie Pretty Good Privacy (PGP) oder GNUPG erfolgen muss.[1572] Der Arbeitnehmer hat durch das Angebot von Verschlüsselungssoftware wie GNUPG die Möglichkeit zum effektiven Selbstdatenschutz,[1573] da ihm hier die anonyme Nutzung ermöglicht wird.

[1569] Dieses Verhältnis zwischen VPN-Auftraggeber und Betroffenem wird allerdings erst im Anschluss an diese Ausführungen im vierten Abschnitt untersucht (siehe S. 380 ff.)
[1570] Siehe S. 320 ff./339 ff.
[1571] Vgl. zur privaten Verschlüsselung der E-Mails von Arbeitnehmern auch Rieß in: Roßnagel, Handbuch Datenschutzrecht, 6.4 Rn. 27.
[1572] Siehe zu PGP S. 275 sowie Däubler, Internet und Arbeitsrecht, Rn. 44.Siehe für nähere Informationen zu GNUP http://www. Gnupg.org.
[1573] Zur Bedeutung des Selbstdatenschutzes siehe auch Weichert, NJW 2001, 1463, 1466. Siehe S. 276 in dieser Arbeit zur Frage, inwieweit eine Informationspflicht über die Verwendung von PGP oder GNUPP aufgrund ihrer Bekanntheitsgrades (noch) erforderlich ist.

Solche so genannten Private Enhancing Technologies (PET) sind im Internet von großer Bedeutung.[1574]

Zu berücksichtigen ist darüber hinaus, dass der Arbeitgeber nicht nur die Möglichkeit hat, seine Mitarbeiter über die Verschlüsselung zu informieren, sondern darüber hinaus zur Verschlüsselung privater E-Mails ausdrücklich aufzufordern. Ein Verschlüsselungsverbot wäre im Übrigen ohnehin ein unzulässiger Eingriff in die Persönlichkeitssphäre des Arbeitnehmers.[1575] Fraglich ist in diesem Zusammenhang jedoch, ob der Arbeitgeber im Umkehrschluss ohne weiteres davon ausgehen darf, dass die Nichtnutzung der von ihm angebotenen und zur Verfügung gestellten Verschlüsselungssoftware bzw. der Verzicht des Arbeitnehmers auf Verschlüsselung ein umfassendes Protokollierungs- und Einsichtsrecht der **versendeten** E-Mails zur Folge hätte.[1576] Ist es dann in diesem Fall „Pech" des Arbeitnehmers, die seitens des Arbeitgebers zur Verfügung gestellte Verschlüsselungssoftware nicht genutzt zu haben? Nach der hier vertretenen Auffassung kann sich diese Frage im Übrigen lediglich stellen, sofern der Arbeitnehmer in die Kenntnisnahme seiner dienstlichen E-Mails durch den Arbeitgeber (freiwillig) eingewilligt hat.[1577]

Richtigerweise muss aber ein Eingriff in die Persönlichkeitsrechte des Arbeitnehmers (*allerdings unter ausdrücklichem Verweis auf die nachfolgend dargestellten Einschränkungen und insbesondere der Konsequenz für die Praxis)*[1578] verneint werden. Ein Arbeitnehmer kann selbst die Kontrolle darüber ausüben, ob seine Kommunikation dem Zugriff seines Arbeitgebers ausgesetzt wird oder nicht. Denn er hat die Formulierung der E-Mails in der Hand und könnte den privaten Teil separat formulieren. Entsprechendes gilt für geschäftlich motivierte E-Mail, die private Komponenten aufweisen.[1579]

[1574] Hornung, MMR 2004, 3, 7.
[1575] Däubler in: Ahrens/Donner/Simon, Arbeit-Umwelt, 2001, S. 1, 4. Siehe außerdem Däubler, Gläserne Belegschaften?, Rn. 353.
[1576] Vgl. S. 321 ff. (wo allerdings ebenso auf die Einschränkung der Verhaltens- und Leistungskontrolle verwiesen wurde).
[1577] Vgl. S. 361.
[1578] Vgl. S. 367 ff. zu den „persönlich-dienstlichen" E-Mails sowie den eingehenden E-Mails.
[1579] Vgl. Fn. 1155 sowie Rosen, The unwanted gaze, The destruction of privacy in America, S. 76 mit dem Hinweis, dass insbesondere durch die Bereitstellung des E-Mail-Accounts die private Kommunikation zwischen den Mitarbeitern ersetzt wird.

Hier kommt es selbstverständlich ebenso auf die einfache Handhabung der Verschlüsselungssoftware an. Produkte wie GNUPG oder PGP überfordern allerdings regelmäßig den Benutzer in der Anwendung nicht und erlauben eine einfache Bedienbarkeit.[1580] Probleme der Nutzer bei der Anwendung von Standardverschlüsselungsprogrammen können nur dann zu Lasten des Arbeitgebers gehen, sofern dieser sich nicht um eine ausreichende Einweisung seiner Mitarbeiter bemüht hat. Unterlässt er daher entsprechende Schulungs- oder Einweisungsmaßnahmen seiner Mitarbeiter, ist von einem Verbot der Einsichtnahme von privaten E-Mails auszugehen. Zu berücksichtigen ist in diesem Kontext ebenso, dass ein Mindestmaß an Eigenverantwortung dem Arbeitnehmer zumutbar ist. Ist dieser trotz Einweisung nicht in der Lage, die Verschlüsselungssoftware zu bedienen, kann er sich andere Alternativen überlegen. Beispielsweise ist die ausdrückliche Kennzeichnung der E-Mail „als privat“ möglich, so dass dem Arbeitgeber ebenso das Einsichtsrecht untersagt wäre. Darüber hinaus gibt es heute vielfältige Möglichkeiten, sich über das Internet in einen privaten „Web-Mail-Account“ einzuwählen. Das Entgegenkommen des Arbeitgebers, den geschäftlichen E-Mail-Account privat nutzen zu dürfen (anstatt ein ausdrückliches Verbot auszusprechen), kann so Rechnung getragen werden. Dies steht allerdings insgesamt unter dem Vorbehalt, dass der Arbeitgeber die Arbeitnehmer deutlich darüber informiert hat, dass er auf unverschlüsselte oder nicht als privat gekennzeichnete versendete E-Mails grundsätzlich Zugriff nehmen darf.

Stellt daher der Arbeitgeber Verschlüsselungsangebote bereit und macht ausdrücklich auf deren Verwendung für private Kommunikation aufmerksam, so ist der Arbeitnehmer angehalten, diese zu nutzen und sein Kommunikationsverhalten beim Verfassen einer E-Mail danach auszurichten. Bei „persönlich-dienstlichen“ E-Mails innerhalb des Unternehmens (beispielsweise wenn der Werksarzt dem Mitarbeiter eine Mitteilung schreibt) muss der Arbeitgeber darüber hinaus an den jeweiligen Absender die Anweisung erteilen, solche Schreiben grundsätzlich verschlüsselt oder aber auf

[1580] Zu PGP und GNUPG siehe auch die Ausführungen unter http://www.bsi.de/gshb/deutsch/m/m05063.html.

dem Postweg zu versenden. [1581] Dies stellt insoweit keine unzulässige Abwälzung von datenschutzrechtlichen Pflichten auf den Arbeitnehmer dar. Denn als Alternative käme in Betracht, dass der Arbeitgeber unterschiedliche Datenverarbeitungssysteme einsetzt und dem Nutzer zwei unterschiedliche E-Mail-Adressen, eine private und eine dienstliche bereit stellt, oder den Arbeitnehmer verpflichtet, seinen privaten E-Mail-Verkehr entsprechend zu kennzeichnen.[1582] In diesen Fällen müsste sich der jeweilige Arbeitnehmer aber ebenso eigenverantwortlich um seine datenschutzrechtlichen Interessen kümmern und private Kommunikation von dienstlicher Kommunikation trennen. Daher ist es insgesamt nicht „arbeitnehmerlastig“, sofern die Arbeitgeber angehalten sind, private E-Mails zu verschlüsseln.
Der Arbeitgeber darf dann allerdings nicht die Anzahl der durchschnittlichen privaten E-Mails auswerten und insoweit keine Leistungskontrolle vornehmen.

Eine grundsätzlich andere Beurteilung ergibt sich jedoch bezüglich **eingehender** E-Mails. Dies gilt unabhängig davon, ob private E-Mail-Kommunikation erlaubt oder seitens des Arbeitgebers ausdrücklich verboten ist.[1583] In diesem Zusammenhang stellt sich insbesondere das Problem der geschäftlich motivierten E-Mail mit privatem Inhalt. Hier ist nicht ausgeschlossen, dass dies den Arbeitnehmer im Einzelfall in „unangenehme“ Situationen bringen könnte. Ein Beispiel wäre eine geschäftliche E-Mail unter Bezugnahme auf einen erfolgreichen Vertragsabschluss. Dies könnte den Arbeitnehmer dann in peinliche Lage bringen, wenn der Geschäftspartner in einer „PS-Zeile“ seine Hoffnung zum Ausdruck bringt, dass es diesem nach der ausgiebigen Feier des Geschäftsabschlusses in der Bar XY wieder besser geht. Unter diesem Blickwinkel bliebe nur die Möglichkeit, dem Arbeitgeber hinsichtlich eingehender E-Mails die Zugriffsrechte vollständig zu versagen. Ob dies allerdings eine rechtliche Anforderung darstellt, kann nur mit Sicht auf die „Sozialüblichkeit“ wie folgt entschieden werden:

[1581] Siehe zur Privatnutzung aus dienstlichem Anlass Däubler, Internet und Arbeitsrecht, Rn. 176; Däubler, K&R 2000, S. 323, 324. Siehe aber auch zum Persönlichkeitsrecht des Empfängers die nachfolgende Darstellung der Problematik „**eingehende** E-Mails“.
[1582] Siehe hierzu auch Abel, Praxishandbuch, IT-Know-How für den Datenschutzbeauftragten, Teil 7/3.2 S.3. Vgl. zu der Möglichkeit der Zuweisung von einer privaten und einer dienstlichen E-Mail-Adresse auch Gola, MMR 1999, 322, 326.
[1583] Vgl. im Übrigen zu den arbeitsrechtlichen Konsequenzen beim privaten Surfen am Arbeitsplatz die Ausführungen sowie den Rechtssprechungsüberblick bei Ernst, DuD 2006, S. 223 ff.

Zurzeit ist es gebräuchlich, dass geschäftliche E-Mails sehr häufig private Komponenten aufweisen. Die Sachlage ist anders als im Rahmen von brieflicher Kommunikation zu beurteilen, die im Regelfall wesentlich förmlicher formuliert ist. So würde beispielsweise niemand einen Geschäftsbrief mit „Hallo" beginnen oder humorvolle Äußerungen einfließen lassen (oftmals mit „Smiley" versehen).[1584] Allerdings ist dies im E-Mail-Verkehr sehr üblich, meist schon nach wenigen Kontakten.

Dies bedeutet aber im Umkehrschluss, dass der Arbeitnehmer auf Formulierungen und das E-Mail-Kommunikationsverhalten des Absenders (anders als im obigen Beispielsfall des Werkarztes) keinen Einfluss nehmen kann. Dennoch können laxe Formulierungen des Absenders ein „bestimmtes Bild" auf den Empfänger (Arbeitnehmer) sowie auf dessen Persönlichkeit werfen. Insbesondere ist zu berücksichtigen, dass der Absender nicht unbedingt davon ausgeht, dass beim Empfänger die private E-Mail-Nutzung verboten ist.

Dementsprechend ist bezüglich sämtlicher eingehender E-Mails eine abweichende Auffassung gerechtfertigt und Zugriffsrechte müssen bei eingehenden E-Mails auch bei einem ausdrücklichen Verbot der privaten E-Mail-Nutzung ausgeschlossen sein.

In praktischer Hinsicht bedeutet dies eine erhebliche Ausweitung der Pflichten des Arbeitgebers, da damit das Verbot des Zugriffs auf sämtliche eingehende sowie ausgehende E-Mails verbunden sein kann, sofern systemtechnisch keine eindeutige Trennung der E-Mail-Postfächer möglich ist.[1585] Zu berücksichtigen ist insbesondere, dass eingehende E-Mails oftmals als Antwort und Reaktion formuliert sind und entweder der gesamte vorherige E-Mail-Verkehr angehängt ist oder sich deren Inhalt aus dem Kontext ergibt.

[1584] Vgl. auch Däubler, Internet und Arbeitsrecht, Rn. 248; Ernst, NZA 2002, 585, 589.

[1585] Regelmäßig findet mittels der E-Mail-Software (z.B. Outlook) automatisch eine Verknüpfung der Daten im Posteingangsordner und Postausgangsordner statt. Vgl. hierzu auch Tanenbaum, Computernetzwerke, S. 643.

cc. Auskunfts- und Überwachungsmaßnahmen

Diese Verpflichtungen können allein gegenüber Mitarbeitern des VPN-Auftraggebers in Betracht kommen, da der VPN-Auftraggeber einem externen Nutzer regelmäßig keinen E-Mail-Account zur Verfügung stellen wird.
Bei der Bereitstellung des Zusatzdienstes E-Mail scheiden diese Verpflichtungen allerdings auch gegenüber Mitarbeitern im Falle von dienstlicher Kommunikation aus, da lediglich Anbieter von *geschäftsmäßig* erbrachten Telekommunikationsdiensten im Sinne der TKÜV[1586] oder gemäß § 100b Abs. 3 Satz 1 der Strafprozessordnung (StPO), des § 2 Abs. 1 Satz 3 des Artikel 10-Gesetzes (G-10-Gesetz) des § 23a Abs. 1 S. 1 des Zollfahndungsdienstegesetzes oder nach Landesrecht auf Anordnung zur Auskunft über verarbeitete Daten verpflichtet sind. Bei dienstlich motivierter E-Mail-Kommunikation sind die Mitarbeiter jedoch keine Dritten gemäß § 3 Nr. 10 TKG.[1587]

Zu berücksichtigen ist aber, dass Auskunfts- und Überwachungsmaßnahmen bei privater E-Mail-Kommunikation in Betracht kommen können. In diesem Falle wäre der VPN-Auftraggeber bei richterlicher Anordnung gemäß §§ 100 g, h StPO insbesondere zur Herausgabe der Kommunikation verpflichtet. Umso wichtiger wäre es für den Datenschutz des Arbeitnehmers daher, seine privaten E-Mails zu verschlüsseln. Denn der VPN-Auftraggeber könnte in diesem Falle lediglich die verschlüsselte Kommunikation bereitstellen.
Im Falle der „persönlich-dienstlich“ *versendeten* E-Mails besteht die Besonderheit, dass der Arbeitgeber auf diese Zugriff nehmen darf, sofern er den Mitarbeitern ausdrücklich zur Verschlüsselung auffordert und ihn in die Handhabung der Verschlüsselungssoftware entsprechend einweist. Damit erbringt er gegenüber den Mitarbeitern keinen geschäftsmäßigen Telekommunikationsdienst und ist nicht zur Auskunft verpflichtet.[1588]
Da die „persönlich-dienstlich“ *eingehenden* E-Mails allerdings insgesamt wie private Kommunikation behandelt werden und damit ein geschäftsmäßig

[1586] Zur TKÜV siehe S. 12 und Fn. 46.
[1587] Siehe zum Begriff des Dritten S. 320.
[1588] Siehe die Ausführungen auf S. 367 ff.

erbrachter Telekommunikationsdienst vorliegt,[1589] ist von der Anordnung (aufgrund der Verknüpfung dienstlicher und privater Komponenten in der E-Mail) zwangsläufig ebenso die Kommunikation erfasst, die den VPN-Auftraggeber bzw. Arbeitgeber betrifft. Ob diese staatlichen Maßnahmen damit zugleich in Grundrechte des VPN-Auftraggebers eingreifen können, ist jedoch nicht Gegenstand der Betrachtung in dieser Arbeit.

b. E-Mail-Kommunikationspartner

Die folgenden Ausführungen befassen sich mit den datenschutzrechtlichen Pflichten des VPN-Auftraggebers im Verhältnis zu seinem E-Mail-Kommunikationspartner bzw. Kommunikationspartner seines Arbeitnehmers, der ebenso als Nutzer des E-Mail-Dienstes qualifiziert wurde.[1590] Es wird hierbei davon ausgegangen, dass dieser E-Mail-Kommunikationspartner kein Mitarbeiter des VPN-Auftraggebers ist (dessen Rechte gerade gesondert geprüft worden sind).

Der VPN-Auftraggeber ist im Verhältnis zu diesem Nutzer, an den er eine E-Mail versendet, kein Telediensteanbieter gemäß § 2 Abs. 2 Nr. 1 TDG. [1591] Mangels Angebot eines Teledienstes kommen infolgedessen keine Löschungsverpflichtungen gemäß § 6 Abs. 4 TDDSG in Betracht, wonach dem Diensteanbieter nur gestattet wäre, Daten die sich auf die näheren Daten der E-Mail, wie E-Mail-Adresse, Datum, Uhrzeit oder Inhalt beziehen, über das Ende des Nutzungsvorgangs hinaus zu verarbeiten und zu nutzen, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind.[1592]
Ebenso wenig findet dass TDDSG Anwendung, sofern ein solcher Nutzer eine E-Mail an den VPN-Auftraggeber zurücksendet und dabei Daten auf dem Rechner des VPN-Auftraggebers entstehen und gespeichert werden, die sich auf die näheren Daten der E-Mail, wie E-Mail-Adresse, Datum, Uhrzeit oder Inhalt beziehen. In diesem Falle wäre der VPN-Auftraggeber von vorneherein kein Telediensteanbieter gemäß § 2 Abs. 2 Nr. 1 TDG, da er selbst keine

[1589] Siehe S. 368.
[1590] Siehe zum Begriff des Nutzers S. 83 ff. sowie S. 302.
[1591] Vgl. oben S. 315 ff.
[1592] Dix/Schaar in: Roßnagel, Recht der Multimedia-Dienste, § 6 TDDSG Rn. 149 ff.

Inhalte anbietet, sondern vielmehr die Inhalte des Nutzers in Anspruch nimmt. In diesem Sinne wäre er also ebenso Nutzer eines Dienstes.
Zur Vereinfachung soll aber im Folgenden als Nutzer nur der Kommunikationspartner und nicht der VPN-Auftraggeber bezeichnet werden.

Aufgrund des Exklusivitätsverhältnisses[1593] ist im Hinblick auf datenschutzrechtliche Pflichten das BDSG anwendbar.
Dies bedeutet, dass der VPN-Auftraggeber grundsätzlich sowohl beim Empfang als auch beim Versand einer E-Mail sämtliche damit verbundene[1594] und auf seinem Rechner angefallene Daten, wie E-Mail-Adresse, Datum, Uhrzeit oder Inhalt[1595] vollumfänglich speichern darf, soweit nicht § 35 BDSG, insbesondere § 35 Abs. 2 Nr. 3 BDSG, entgegensteht. Regelmäßig findet mittels der E-Mail-Software (z.B. Outlook) automatisch eine Verknüpfung der Daten im Posteingangsordner und Postausgangsordner statt.

aa. Datenvermeidung

Die E-Mail-Adresse des E-Mail-Kommunikationspartners bzw. Nutzers stellt für den VPN-Auftraggeber ein personenbezogenes Datum gemäß § 3 Abs. 1 BDSG dar, sofern der E-Mail-Kommunikationspartner bzw. Nutzer bestimmbar ist.[1596] Dies wird regelmäßig aufgrund des gegenseitigen Austausches von Visitenkarten im Vorfeld der Kommunikation der Fall sein.[1597]

[1593] Siehe S. 92.
[1594] Regelmäßig findet mittels der E-Mail-Software (z.B. Outlook) automatisch eine Verknüpfung der Daten im Posteingangsordner und Postausgangsordner statt. Vgl. hierzu auch Tanenbaum, Computernetzwerke, S. 643.
[1595] Hiervon zu unterscheiden ist das Fernmeldegeheimnis gemäß § 88 TKG, welches zwar den Inhalt der Telekommunikation schützt, aber hier nicht in Betracht kommt, da der VPN-Auftraggeber im Verhältnis zum Nutzer kein Telekommunikationsanbieter ist. Auch hier ist wiederum auf das „richtige“ Verhältnis abzustellen. Inhaltsdaten bei E-Mail unterfallen gegenüber dem Provider dem § 88 TKG, gegenüber dem jeweiligen Nutzer dem BDSG (siehe zu den Inhaltsdaten auch S. 105 und S. 347, siehe aber auch Schaffland/Wiltfang, § 1 BDSG Rn. 69).
[1596] Zur Bestimmbarkeit siehe oben S. 92 ff. und Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 107.
[1597] Bei der E-Mail-Adresse handelt es sich im Übrigen nicht ohne weiteres um ein allgemein zugängliches Datum handelt. Allgemein zugängliche Quellen sind etwa Zeitungen, Telefonbücher, das Internet (Gola/Schomerus, BDSG, § 28 BDSG Rn. 45). Eine E-Mail-Adresse einer Person ist aber nicht zwangsläufig auffindbar. Zwar gibt es Suchdienste im Internet (Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 94), aber nicht jeder Nutzer hat sich dort registrieren lassen (siehe auch Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 108).

Beim Versand einer E-Mail an einen E-Mail-Kommunikationspartner bzw. Nutzer werden die mit der E-Mail-Adresse verknüpften Daten der E-Mail-Kommunikation, wie Datum und Uhrzeit der Versendung sowie Inhalt, auf dem Rechner des VPN-Auftraggebers gespeichert und stellen damit nicht nur personenbezogene Daten des VPN-Auftraggebers sondern ebenso des E-Mail-Kommunikationspartners bzw. Nutzers dar.
Eine Löschung der E-Mail-Adresse sowie der anderen Daten (z.B. Inhalt) kommt nach § 35 Abs. 2 Nr. 3 BDSG in Betracht, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, etwa bei völligem Abbruch der geschäftlichen Verbindung oder bei abschließender Beantwortung Anfrage des E-Mail-Kommunikationspartners bzw. Nutzers.[1598]

Wird der VPN-Auftraggeber vom E-Mail-Kommunikationspartner bzw. Nutzer per E-Mail kontaktiert, stellt dessen E-Mail-Adresse regelmäßig ein personenbezogenes Datum dar, da entweder der E-Mail-Kommunikationspartner bzw. Nutzer dem VPN-Auftraggeber bekannt ist, der komplette Name des Nutzers in der E-Mail-Adresse enthalten ist oder als Zusatz übermittelt wird.[1599] In diesem Fall wird aber selbst bei einem Fantasienamen[1600] in der E-Mail-Adresse die Bestimmbarkeit im Sinne von § 3 Abs. 1 BDSG gegeben sein, da die Versendung einer E-Mail an den VPN-Auftraggeber nur dann sinnvoll ist, sofern sich die Person „hinter“ der E-Mail-Adresse identifiziert.[1601]

[1598] Siehe hierzu aber auch Gola/Schomerus, BDSG, § 35 BDSG Rn. 13, wonach damit nicht gemeint ist, dass der ursprüngliche Speicherungszweck entfallen ist. Denn sofern sich nach Wegfall des ursprünglichen Speicherungszwecks (z.B. Abwicklung eines Kaufvertrages mit einem Versandhauskunden) eine neue Legitimationsgrundlage für die weitere Speicherung ergibt (z.B. Zusendung von Werbematerial), so besteht hinsichtlich der insoweit erforderlichen Daten keine Löschungsverpflichtung. Entsprechendes kann daher auch für die Speicherung der E-Mail-Adresse gelten, sofern etwa der Dritte in die Zusendung von Werbe-E-Mails eingewilligt hat (§ 7 Abs. 3 UWG n.F. ist nur anwendbar, wenn ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat, siehe § 7 Abs. 3 Nr. 1 UWG. Der BGH hatte hierzu entscheiden, dass unverlangte E-Mail-Werbung sittenwidrig ist (vgl. BGH, CR 2004, 445 ff.; zur Wettbewerbswidrigkeit von Telefon- Fax- und E-Mail-Werbung siehe außerdem die Stellungnahme von Wülfing, ITRB 2004, 152, 152).
[1599] Siehe auch Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 49 und dem Hinweis, dass die Domain Auskünfte über den Beruf des Nutzers geben kann. Sofern die Domain auf ein Unternehmen registriert ist, spreche alles dafür, dass der Nutzer für diese Firma tätig ist, gehöre sie zu einer Universität, so sei der Nutzer wahrscheinlich Student. Siehe außerdem Schmitz, TDDSG und das Recht auf informationelle Selbstbestimmung, S. 94.
[1600] Vgl. Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 108.
[1601] Damit werden so genannte Spam-Mails regelmäßig anonym sein, wobei diese der Nutzer jedoch Gründen regelmäßig „freiwillig“ löschen wird.

In der Praxis kann sich für den VPN-Auftraggeber die Löschung der E-Mail-Kommunikation schwierig gestalten. Wenn es sich um dienstliche und damit um „seine" Kommunikation handelt, ist der VPN-Auftraggeber derjenige, der durch entsprechende dienstliche Anweisungen oder Verpflichtungen im Arbeitsvertrag dafür Sorge tragen muss, dass seine Mitarbeiter den gesetzlichen Löschungsverpflichtungen nachkommen.[1602] Dem VPN-Auftraggeber wird es zum einen aus zeitlichen und inhaltlichen Gründen regelmäßig nicht möglich sein, die E-Mails selbst zu löschen. Zum anderen hätte der VPN-Auftraggeber ohnehin nur eingeschränkte Prüfungs- bzw. Einsichtsrechte,[1603] so dass die Mitarbeiter selbständig über die Notwendigkeit der Speicherung entscheiden müssten. Dies ist jedoch aus dem Grunde problematisch, da die Mitarbeiter außerdem eigenständig entscheiden müssten, welche E-Mails privaten und welche ausschließlich geschäftlichen Charakter haben, da im Privatbereich gemäß § 3 Abs. 2 Nr. 3 BDSG datenschutzrechtlichen Regelungen von vorneherein keine Anwendung finden. Hier kann aber im Einzelfall eine eindeutige Differenzierung ebenso schwierig sein.[1604]
Es empfiehlt sich daher für den VPN-Auftraggeber, entweder die private Nutzung des E-Mail-Accounts vollständig zu untersagen, oder aber Systeme einzusetzen, die eine getrennte Verarbeitung der E-Mails erlauben.[1605]

Darüber hinaus könnte bei Einsichtnahme in den (inhaltlichen) E-Mail-Verkehr durch den VPN-Auftraggeber die Interessenlage des E-Mail-Kommunikationspartners vergleichbar zu der eines Arbeitnehmers sein. [1606] Daher ist fraglich, ob ebenso im Verhältnis zum E-Mail-Kommunikationspartner

[1602] Darüber hinaus sind hier gleichermaßen die Aufbewahrungspflichten aus dem Handelsgesetzbuch (HGB) und der Abgabenordnung (AO) zu berücksichtigen. Siehe hierzu Abel, Praxishandbuch Datenschutz Teil 6/7.6.1 Seite 3 mit dem Hinweis, dass bei E-Mail-Kommunikation Archivierungspflichten gemäß § 257 Abs. 1 HGB und § 147 Abs. 1 und 3 AO in der Regel für sechs Monate (gewöhnliche geschäftsrelevante Mails) bzw. zehn Jahre (Mails mit Bilanzwirksamkeit wie Rechnungen) bestehen. Vgl. außerdem Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 79 in Bezug auf die ausgelagerte Datenverarbeitung. Darüber hinaus sind hier gleichermaßen die Aufbewahrungspflichten aus dem Handelsgesetzbuch (HGB) und der Abgabenordnung (AO) zu berücksichtigen.
[1603] Vgl. oben S. 357 ff. und S. 367 ff.
[1604] Siehe zu den persönlich-dienstlichen E-Mails S. 367 ff, Siehe außerdem Fn. 1155, insbesondere den Hinweis auf Rosen, The unwanted gaze, The destruction of privacy in America, S. 76.
[1605] Siehe außerdem die folgenden Ausführungen auf S. 377 zur unzulässigen Abwälzung von datenschutzrechtlichen Pflichten auf den Arbeitnehmer.
[1606] Siehe S. 357 ff., 361 ff., S. 367 ff. Vgl. S. 361 zur mittelbaren Grundrechtsbindung im Arbeitsverhältnis.

ein Eingriff in dessen Persönlichkeitsrecht bejaht werden könnte, sofern der VPN-Auftraggeber in die E-Mails Einblick nimmt.

Als Normadressat[1607] des BDSG ist der VPN-Auftraggeber grundsätzlich zur Beachtung des Schutzgegenstandes „Persönlichkeitsrecht" verpflichtet[1608] und insoweit ebenfalls mittelbar an die Grundrechte gebunden.[1609] Zu berücksichtigen ist in diesem Zusammenhang außerdem, inwieweit eine nicht ausreichende Transparenz der Datenverarbeitung und damit ein Verstoß gegen das informationelle Selbstbestimmungsrecht vorliegen könnte.[1610] Denn dem E-Mail-Kommunikationspartner bleibt insbesondere bei einer juristischen Einheit regelmäßig verborgen, welchen Personen letztendlich Einsichtsrechte in den E-Mail-Verkehr zustehen: Dem Vorstand, dem Geschäftsführer, dem Leiter einer Abteilung oder nur dem fachlich Vorgesetzten?[1611]

Diese Frage ließe sich zwar intern (im Verhältnis zwischen Arbeitnehmer und Arbeitgeber) durch ein Rollen- und Berechtigungskonzept klären. Im Verhältnis zum E-Mail-Kommunikationspartner fehlt es jedoch an der notwendigen Transparenz bezüglich der Frage, wer die E-Mail „außerdem" lesen darf. Es muss daher aus Sicht des E-Mail-Kommunikationspartners ermittelt werden, ob er in seiner Entscheidungsfreiheit derart beschränkt ist, dass daraus eine Verletzung seines Persönlichkeitsrechts resultieren könnte. Dabei steht zum

---

[1607] Gola/Schomerus, BDSG, § 1 BDSG Rn. 19.

[1608] Vgl. Gola/Schomerus, BDSG, § 1 BDSG Rn. 6 zum Schutzgegenstand des BDSG. In § 1 Abs. 1 BDSG ist das Ziel normiert, das Vorrecht des Betroffenen zu garantieren, so dass dieser selbst darüber entscheiden kann, wer unter welchen Umständen und für welchen Zweck auf seine Daten zugreifen darf (vgl. hierzu Simitis in: Simitis, BDSG-Kommentar, § 1 BDSG RN. 25, der darauf verweist, dass sich trotz anders lautendem Wortlaut dieser Anknüpfungspunkt an das informationelle Selbstbestimmungsrecht des Betroffenen im Sinne der Bundesverfassungsgerichtsentscheidung durchgesetzt hat).

[1609] Siehe zur mittelbaren Drittwirkung der Grundrechte Pieroth/Schlink, Grundrechte, Rn. 173 ff., insbesondere Rn. 183 mit dem Hinweis, dass die Bedeutung der mittelbaren Drittwirkung vor allem darin zu sehen ist, dass sie auch unter den Bedingungen der modernen hochkomplexen Industriegesellschaft Freiheit und Gleichheit zu wahren hilft. Die Chancengleichheit kann ebenso durch die Ausübung privater wirtschaftlicher und sozialer Macht beseitigt oder gefährdet sein. Vgl. S. 361 zur mittelbaren Grundrechtsbindung im Arbeitsverhältnis.

[1610] Das informationelle Selbstbestimmungsrecht findet seine Grundlage in Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG und gewährt dem Betroffenen das Recht, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (BVerfGE 65, 1, 48).

[1611] Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Datenweitergabe seiner persönlichen Daten voraus (vgl. Gola/Schomerus, BDSG, § 1 BDSG Rn. 10 sowie Gola/Schomerus, BDSG, § 33 BDSG Rn. 1 mit dem Hinweis, dass Transparenz der Datenverarbeitung zu den verfassungsrechtlich gewährleisteten Grundpositionen des Betroffenen zählen). Siehe zum Zweckbindungsgrundsatz v.Zezschwitz in: Roßnagel, Handbuch Datenschutzrecht, 3.1 Rn. 3 ff. Der Zweckbindungsgrundsatz beinhaltet, dass dem Einzelnen möglichst genau bekannt ist, „wer was wann und bei welcher Gelegenheit über ihn weiß" (v.Zezschwitz in: Roßnagel, Handbuch Datenschutzrecht, 3.1 Rn. 4).

einen die Frage im Mittelpunkt, von welchem Sachverhalt er im Rahmen geschäftlicher Kommunikation üblicherweise ausgeht und auch ausgehen darf, und zum anderen ob eine „faktische Asymmetrie“ zwischen den Interessen des VPN-Auftraggebers und des E-Mail-Kommunikationspartners vorliegen könnte.[1612] Hiervon ausgehend ergibt sich folgende Bewertung:
Schreibt der E-Mail-Kommunikationspartner beispielsweise eine E-Mail an eine offizielle Info-Adresse eines Unternehmens (info@unternehmen.de) so muss er damit rechnen, dass seine Anfrage von einer nicht näher bestimmten Anzahl von Personen gelesen und bearbeitet wird. Steht er jedoch in regelmäßigen E-Mail-Kontakt mit einem Mitarbeiter des Unternehmens, geht er nicht unbedingt davon aus, dass die Korrespondenz mitgelesen wird (auch wenn er mit dem VPN-Auftraggeber im rechtlichen Sinne ein Geschäft abschließt).
Andererseits sollte jedem E-Mail-Nutzer die „bcc“-Funktion des E-Mail-Dienstes bekannt und der Umstand bewusst sein, dass seine E-Mails als Teil der geschäftlichen Dokumentation von anderen gelesen (z.B. Urlaubsvertretung) und beispielsweise in ausgedruckter Form in Akten archiviert werden (können). Aus diesem Grunde kann unter Umständen sein Recht auf Datenlöschung gemäß § 35 Abs. 2 BDSG, aber nicht sein Recht auf informationelle Selbstbestimmung verletzt sein. Denn der Verfasser einer E-Mail kann sein Kommunikationsverhalten stets diesen Umständen entsprechend anpassen kann und er kann daher darauf Einfluss nehmen, welche Informationen über ihn gespeichert werden. Es liegt (anders als im Arbeitsverhältnis) folglich keine Verletzung des Persönlichkeitsrechts des E-Mail-Kommunikationspartners vor. Insbesondere ist hier auch kein ungleiches Machtverhältnis zwischen E-Mail-Kommunikationspartner und VPN-Auftraggeber gegeben, welches eine andere Bewertung rechtfertigen könnte.

Bei privaten E-Mails ist ein Eingriff in das Persönlichkeitsrecht des E-Mail-Kommunikationspartners bei Kenntnisnahme des Inhalts durch den VPN-Auftraggeber ebenso zu verneinen.[1613] Der E-Mail-Kommunikationspartner kann sich frei dazu entscheiden, an eine geschäftliche E-Mail-Adresse zu schreiben und muss damit rechnen, dass ggf. anderen Personen Zugriffsrechte

[1612] Vgl. auch Pieroth/Schlink, Grundrechte, Rn. 183.
[1613] Vgl. aber die Ernst, NZA 2002, 585, 589, der davon ausgeht, dass die Persönlichkeitsrechte des Absenders bzw. E-Mail-Kommunikationspartners betroffen sind.

auf den entsprechenden E-Mail-Account durch den Nutzer selbst eingeräumt sind (unter anderem dem Sekretariat, der Urlaubsvertretung, etc.). Daher liegt hier kein Eingriff in das Persönlichkeitsrecht des E-Mail-Kommunikationspartners vor, da dieser in seiner Entscheidungsfreiheit insgesamt nicht beeinträchtigt ist. Ihm ist –wie bei einer Postkarte bekannt– dass seine Privatsphäre nicht zwangsläufig gewahrt wird.

Gemäß § 35 BDSG und im Sinne einer effektiven Datenvermeidung gemäß § 3a BDSG ist es nichtsdestotrotz insgesamt erforderlich, dass stets geprüft wird, inwieweit die Daten des geschäftlichen E-Mail-Verkehrs sowie dessen Inhalt benötigt werden und deren Speicherung erforderlich ist.[1614] Hier besteht die Schwierigkeit, dass der Arbeitgeber einerseits für den Datenschutz seines E-Mail-Kommunikationspartners (aus BDSG) verantwortlich ist und diese Pflichten nicht auf den Arbeitnehmer abwälzen darf.[1615] Andererseits sind ihm aber jegliche Einsichtsrechte in die geschäftliche Kommunikation verwehrt, sofern der Arbeitnehmer hierin nicht ausdrücklich einwilligt.[1616] Daher muss in diesem Fall gelten, dass dem Arbeitnehmer zwar gemäß seiner arbeitsvertraglichen Pflichten obliegt, eine „ordentliche" Dokumentation der geschäftlichen Korrespondenz vorzunehmen.[1617] Er kann jedoch gegenüber dem E-Mail-Kommunikationspartner nicht „selbständig" aus datenschutzgesetzlichen Gesichtspunkten zur Löschung verpflichtet sein.

bb. Unterrichtungspflichten

Fraglich ist, inwieweit ein VPN-Auftraggeber verpflichtet ist, den E-Mail-Kommunikationspartner bzw. Nutzer über den Umfang der Speicherung der von diesem versendeten oder empfangenen E-Mail zu unterrichten. Zwar werden E-Mail-Adressen zumeist im Vorfeld einer Kommunikation ausgetauscht, so dass dem Versender bewusst ist, dass die E-Mail, die er an den VPN-Auftraggeber

[1614] Siehe zur Erforderlichkeit S. 98.
[1615] Siehe zur Verantwortung des Arbeitgebers im Rahmen von Telearbeit: Wedde, Telearbeit, S. 133 mit dem Hinweis, dass der Arbeitgeber für die Einhaltung der gesetzlichen Vorgaben allein verantwortlich ist und sich von dieser Verantwortung nicht durch entsprechende Vereinbarungen mit den Beschäftigten freimachen kann.
[1616] Vgl. S. 357 ff.
[1617] Vgl. S. 360 ff. unter Hinweis auf Schaub, Arbeitsrechts-Handbuch, § 53 Rn. 14 zur Nebenpflicht des Arbeitnehmers.

übersendet, oder die E-Mail, die er von dem VPN-Auftraggeber erhält, auch auf dessen Rechner gespeichert wird, so dass von einer Einwilligung gemäß § 4a Abs. 1 S. 3 BDSG auszugehen ist.[1618]

Jedoch ist zu berücksichtigen, dass der E-Mail-Kommunikationspartner bzw. Nutzer keinen Einblick darin hat, für welche Dauer die Daten auf den Rechnern des VPN-Auftraggebers gespeichert werden. Gemäß § 34 BDSG steht ihm zwar grundsätzlich ein Auskunftsrecht zu. Dennoch sollten zumindest auf der Website des VPN-Auftraggebers datenschutzrechtliche Regelungen im Hinblick auf den Umgang mit E-Mails, insbesondere bezüglich der Löschung, enthalten sein.[1619] Diese Unterrichtung kommt ebenso im Zusammenhang mit „Info"-E-Mail-Adressen in Betracht, etwa sofern der Unternehmer auf seiner Website Dritte dazu „einlädt", an seine info@unternehmen-x.de Adresse Anfragen in Form von E-Mails zu senden.

Eine gesetzliche Verpflichtung zur Unterrichtung kommt gemäß § 4 Abs. 3 BDSG allerdings lediglich im Hinblick auf die Unterrichtung bezüglich der Kategorien von Empfängern nach § 4 Abs. 3 Nr. 3 BDSG in Betracht, da dem E-Mail- Kommunikationspartner bzw. Nutzer beim Versenden einer E-Mail an den VPN-Auftraggeber dessen Identität im Sinne von § 4 Abs. 3 Nr. 1 BDSG bereits bekannt ist, und er darüber hinaus eine Zweckbestimmung im Sinne von § 4 Abs. 3 Nr. 2 BDSG selbst vornimmt.[1620]

Im Übrigen muss dem E-Mail- Kommunikationspartner bzw. Nutzer die Möglichkeit verbleiben, die Verarbeitung seiner Daten für die Zukunft zu untersagen und die Löschung der Daten zu verlangen.[1621] Auch auf diesen

[1618] Vgl. Gola/Schomerus, BDSG, § 4a BDSG Rn. 6 zur Freiwilligkeit der Einwilligung. Siehe außerdem die Ausführungen zur Einwilligung gemäß § 4a BDSG auf S. 95 in dieser Arbeit.

[1619] Siehe auch Enzmann/Scholz in: Roßnagel, Datenschutz beim Online-Einkauf, S. 75, die darauf verweisen, dass eine gesetzeskonforme Unterrichtung des Nutzers über die angestrebte Datenverarbeitung für einen Anbieter im Internet vergleichsweise leicht zu realisieren ist. Es genügt, wenn der Anbieter eine Website erstelle, in der über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten informiert wird. Der Inhalt einer solchen Seite wird oft auch als Datenschutzrichtlinie oder Datenschutzpolitik bezeichnet (Enzmann/Scholz aaO).

[1620] Vgl. im Übrigen zur Unterrichtung gemäß § 4 TDDSG auch Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 143 mit dem Hinweis, dass die Unterrichtung nicht vor jedem Nutzungsvorgang wiederholt werden muss, sondern der Nutzer nur die Möglichkeit haben muss, die Unterrichtung jederzeit abrufen zu können. Ebenso Rasmussen, CR 2002, 36, 42, die auf die Gesetzesbegründung verweist (Entwurf eines Gesetzes über rechtliche Rahmenbedingung für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz- EGG), Bundestag-Drucksache 14/6098, S. 28).

[1621] Die jederzeitige Widerrufsmöglichkeit der Einwilligung ist Ausdruck der Entscheidungsfreiheit des Nutzers über die Verwendung seiner Daten, wobei sie den Nutzer gleichzeitig vor einer überholt getroffenen Entscheidung schützen soll (Bizer in: Roßnagel,

Umstand sollte der VPN-Auftraggeber auf seiner Website oder aber in einer automatischen Signatur am Ende seiner E-Mails hinweisen.

Eine Unterrichtungsverpflichtung über Verschlüsselung oder gar ein Angebot zur verschlüsselten Übertragung des VPN-Auftraggebers § 109 Abs. 1 TKG unter Berücksichtigung des Artikels 4 der EU-Richtlinie 2002/58/EG ergibt sich jedoch nicht.

Der VPN-Auftraggeber ist im Verhältnis zum E-Mail- Kommunikationspartner kein Anbieter eines Telekommunikationsdienstes gemäß § 3 Nr. 6 TKG. Aus diesem Grunde kommen im Hinblick auf den E-Mail- Kommunikationspartner bzw. Nutzer keine Auskunfts- oder Überwachungsmaßnahmen in Betracht.

Recht der Multimedia-Dienste, § 4 TDDSG Rn. 288). Siehe außerdem zum jederzeitigen Widerrufsrecht S. 417.

4. Abschnitt
Datenschutz des Betroffenen im VPN

Im dritten Abschnitt dieser Arbeit ist Datenschutz in Bezug auf einen *jeweiligen* Nutzers im Verhältnis zum *jeweiligen* Anbieter eines Online-Dienstes untersucht worden. In diesem vierten Abschnitt ist Gegenstand der Betrachtung, welche datenschutzrechtlichen Interessen einer Person zu beachten sind, die nicht selbst als Nutzer aktiv am Kommunikationsvorgang teilnimmt.[1622] Datenschutz spielt dann eine Rolle, wenn personenbezogene Daten dieser Person von VPN-Auftraggeber und Nutzer gemäß § 3 Abs. 4 BDSG verarbeitet oder gemäß § 3 Abs. 5 BDSG innerhalb des VPN genutzt werden. Daher ist der Begriff „Betroffener" gewählt worden, der ebenso der gesetzlichen Definition des § 3 Abs. 1 BDSG entspricht.[1623]

A.
VPN-Auftraggeber - Betroffener

Im Folgenden werden die datenschutzrechtlichen Interessen eines Betroffenen untersucht, die der VPN-Auftraggeber im Zusammenhang mit der Bereitstellung eines VPN zu beachten hat. Im Einzelnen sind dies die rechtlichen Probleme im Rahmen von Telearbeit sowie E-Mail-Nutzung.

I. Telearbeit

Der VPN-Auftraggeber hat bei der Bereitstellung eines VPN in rechtlicher und organisatorischer Hinsicht Anforderungen zu erfüllen, die sich aus dem Kontext der Telearbeit ergeben. Die Organisation der Telearbeit durch den VPN-Auftraggeber muss zum einen den Persönlichkeitsschutz des Telearbeitnehmers „bei der Arbeit" ausreichend berücksichtigen und zum anderen die Daten des Betroffenen, die seitens des Telearbeitnehmers „online" bearbeitet werden, ausreichend schützen.[1624] Die nachfolgenden Ausführungen

[1622] Siehe zum Begriff des Betroffenen S. 85.
[1623] Siehe zum Oberbegriff „Verwendung" für die Verarbeitung und Nutzung Gola/Schomerus, BDSG, § 3 BDSG Rn. 25.
[1624] Siehe hierzu auch Boemke/Ankersen, BB 2000, 1570 ff., zum Schutz der betrieblichen Daten des Arbeitgebers auch S. 1572.

befassen sich mit diesen Schutzmaßnahmen, wobei ebenso die Unterscheidung zwischen „Auftragsdatenverarbeitung“ sowie „Funktionsübertragung“ von besonderer Relevanz ist.[1625]

1. Was ist Telearbeit?

Es existiert bezüglich des Begriffs „Telearbeit“ keine verbindliche Definition, wobei jedoch im Allgemeinen davon alle Tätigkeiten umfasst sind, die räumlich entfernt vom Standort des Arbeit- oder Auftraggebers und unterstützt durch Informations- und Kommunikationstechnologien durchgeführt werden.[1626] Aufgezählt werden hierbei die Telearbeit (im häuslichen Bereich)[1627], entweder in ausschließlicher oder alternierender Form, Telearbeitszentren als regionale Zusammenschlüsse mehrerer Telearbeitsplätze auch von mehreren Verwaltungen oder Unternehmen, die mobile Telearbeit sowie der Zusammenschluss mehrerer räumlich getrennter Selbständiger auf Dauer oder für die Dauer eines Projekts.[1628] Bei Telearbeit handelt es sich um eine Organisationsform und nicht um ein Berufsbild.[1629]

Telearbeit hat insbesondere unter zeitlichen Gesichtspunkten Vorzüge aufzuweisen, da An- und Abfahrtswege entfallen und die Kommunikation der

[1625] Siehe zu diesen Begriffen die Ausführungen bei Müthlein/Heck, Outsourcing, S. 34 ff.
[1626] Eine Auflistung der unterschiedlichen Formen der Telearbeit findet sich bei Däubler, Internet und Arbeitsrecht, Rn. 53. Siehe außerdem Nägele in: Gounalakis, Rechtshandbuch Electronic Business, § 48 Rn. 2 ff.; Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 2; Schlachter in: Noack/Spindler, Unternehmensrecht und Internet. S. 199.
[1627] Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 73 verweist darauf, dass für Telearbeit auch die Begriffe Computerheimarbeit, Teleheimarbeit oder Fernarbeit benutzt werden.
[1628] Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 3. Eine Übersicht zu weiteren Organisationsformen der Telearbeit findet sich in: Basisinformation Telearbeit des Projekts „Online-Forum Telearbeit“, S. 7, wobei hier unter anderem auch der Begriff des „Guerilla“-Teleworkers genannt wird, und damit eine Arbeitsform bezeichnet wird, die meistens von Führungskräften und Spezialisten praktiziert wird, und welche sich immer und überall (ob im Büro, am Wochenende, im Urlaub auf Geschäftsreisen) ins Firmennetz einwählen können. Siehe außerdem Gola/Jaspers, RDV 1998, 243, 245 zu den Erscheinungsformen der Telearbeit. Siehe außerdem zu den unterschiedlichen Varianten der Telearbeit Wedde, NZA 1999, 527, 527; Wedde, Telearbeit, S. 2/3; Haupt/Wollenschläger, NZA 2001, 289, 290/291, Wank, NZA 1999, 2225, 230 sowie Hohmeister/Küper, NZA 1998, 1206, 1206. Der Tarifvertrag über Telearbeit bei der Deutschen Telekom AG/T-Mobile ist im selben Heft auf S. 1214 ff. abgedruckt.
[1629] Siehe Basisinformation Telearbeit des Projekts „Online-Forum Telearbeit“, S. 6. Vgl. außerdem Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 73 mit der Anmerkung, dass es sich bei Telearbeit um eine neue Arbeitsform handelt, bei der die Tätigkeit außerhalb des Betriebs an einem privaten Arbeitsplatz geleistet wird, und zwar in der Regel in der Wohnung des Telearbeitnehmers.

Beschäftigten oder Nutzer untereinander auf diese Weise leichter und schneller gelingen kann.[1630]
Daher ist auch ein VPN unter den Begriff der Telearbeit zu subsumieren. Besondere datenschutzrechtliche Probleme ergeben sich hierbei aufgrund der Beschaffenheit im häuslichen Bereich bei Telearbeit.[1631]

Weiterhin kann Telearbeit aber ebenso im Zusammenhang mit dem Begriff des Outsourcing genannt werden.
Unter Outsourcing ist die Datenverarbeitung durch ein anderes bzw. externes Unternehmen zu verstehen.[1632] Es gibt hierbei im Übrigen kein Konzernprivileg, so dass rechtlich selbständige Unternehmen innerhalb eines Gesamtkonzerns ohne weiteres zur Datenverarbeitung berechtigt wären.[1633] Beim Outsourcing kommt entweder eine Auftragsdatenverarbeitung oder aber eine Funktionsübertragung in Betracht,[1634] so dass die Datenverarbeitung in einem VPN durch Externe (Lieferanten), freie Mitarbeiter, Zweigstellen oder Tochterunternehmen ebenso unter den Begriff des Outsourcing fällt. Diesbezüglich ist also der Regelungsrahmen des BDSG zu beachten.[1635]

So hängt es von der Konkretisierung des Auftrags sowie der Art der „Rollenverteilung“ ab, ob eine Auftragsdatenverarbeitung vorliegt.[1636] Eine Auftragsdatenverarbeitung liegt etwa dann vor, sofern der Dienstleister unselbständig tätig ist und den Weisungen des Auftraggebers unterworfen ist,

---

[1630] Schlachter in: Noack/Spindler, Unternehmensrecht und Internet. S. 199; Hohmeister/Küper, NZA 1998, 1206, 1208. Zu den Vorteilen der Telearbeit von Arbeitnehmern siehe außerdem Wedde, Telearbeit, S. 11/12.
[1631] Vgl. auch Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 8 Fn.14.
[1632] Siehe Klöver/Wedde, CR 1993, S. 93, 94 mit dem Hinweis, dass der Begriff ursprünglich im Datenverarbeitungsbereich geprägt wurde, u.a. für die externe Nutzung von Rechenzentrums- und Netzdiensten. Vgl. zum Outsourcing ebenso Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 89; Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 406 ff. Siehe Büllesbach/Rieß, NVwZ 1995, 444 ff. zum Outsourcing in der öffentlichen Verwaltung im Zusammenhang mit IT-Leistungen.
[1633] Büllesbach, CR 2000, 11, 14; Schaffland/Wiltfang, BDSG, § 27 BDSG Rn. 24; Gola/Schomerus, BDSG, § 27 BDSG Rn. 4.
[1634] Hartig in: Roßnagel, Handbuch Datenschutzrecht, 6.2 Rn. 89; Ulmer, CR 2003, 701, 702. Ebenso Müthlein, RDV 1993, 165, 170, der anmerkt, dass (externes bzw. echtes) Outsourcing lediglich eine moderne Bezeichnung für die Auftragsdatenverarbeitung oder Funktionsübertragung darstellt. Müthlein (aaO) verweist darüber hinaus auf das so genannte „interne Outsourcing“, welches von einer unternehmenseigenen Abteilung oder rechtlich unselbständigen Zweigstelle wahrgenommen wird. Siehe hierzu auch Steding, BB 2001, 1693, 1699.
[1635] Vgl. hierzu Wedde, Telearbeit, S. 128 ff.
[1636] Gola/Schomerus, BDSG, § 11 BDSG Rn. 9. Vgl. auch Wronka, RDV 2003, 132, 133 ff.

quasi als sein verlängerter Arm fungiert, und sich der Auftragsschwerpunkt in erster Linie auf die technische Durchführung der Datenverarbeitung richtet.[1637] Typisches Beispiel für eine Auftragsdatenverarbeitung ist die Beauftragung eines Rechenzentrums mit der Durchführung bestimmter Datenverarbeitungsaufgaben.[1638]

Eine Funktionsübertragung kommt hingegen in Betracht, wenn die Aufgabe des Dienstleisters nicht nur darin besteht, für die Einsatzbereitschaft seines Systems Sorge zu tragen, sondern über die weisungsabhängige technische Datenverarbeitung hinausgeht.[1639] Dies liegt vor, wenn dem Provider bzw. Dienstleister nicht allein die Verarbeitung der Daten übertragen wird, sondern vielmehr eine gesamte Aufgabe, zu deren Erfüllung die Verarbeitung der Daten notwendig ist,[1640] so dass ihm eigene Entscheidungsbefugnisse hinsichtlich des „Wie" und der Auswahl der Daten zustehen, und er selbständig ohne Weisungen des Auftraggebers arbeitet.[1641]

Es ist daher nicht möglich, eine pauschale Aussage dahingehend zu treffen, ob ein Externer, eine Zweigstelle oder das Tochterunternehmen eine Datenverarbeitung nach § 11 BDSG vornimmt oder aufgrund einer Funktionsübertragung selbständig handelnder Dritter ist.[1642] Dies hängt vielmehr vom jeweiligen Einzelfall und der jeweiligen eingeräumten oder im

[1637] Vgl. Kramer/Herrmann, CR 2003, 938, 938; Evers/Keine, NJW 2003, 2726, 2727; Steding, BB 2001, 1693, 1698.

[1638] Steding, BB 2001, 1693, 1698.

[1639] Vgl. hierzu auch Müthlein/Heck, Outsourcing und Datenschutz, S. 34 ff.; Niedermeier/Schröcker, RDV 2001, 90, 92. Steding, BB 2001, 1693, 1699 ff.

[1640] Vgl. Geis, Recht im eCommerce, S. 74, der eine Funktionsübertragung dann annimmt, wenn die Aufgabe zur selbständigen Erledigung übertragen wird und der Datenverarbeiter selbst bestimmen kann, welche Arten personenbezogener Daten gespeichert oder verarbeitet werden. In diesem Sinne ebenso Niedermeier/Schröcker, RDV 2001, 90, 93 und Schneider, Handbuch des EDV-Rechts, Teil B Rn. 448.

[1641] Vgl. Kramer/Herrmann, CR 2003, 938, 939. Wächter, CR 1991, 333, 334 verweist für die Auftragsdatenverarbeitung auf die notwendigen Weisungen des Auftraggebers als „verbindliche Richtschnur" des Handelns des Auftragnehmers. Siehe auch Niedermeier/Schröcker, RDV 2001, 89, 92; v.Westphalen, WM 1999, 1810, 1815.

[1642] Ein Überblick über die Voraussetzungen einer Auftragsdatenverarbeitung in Abgrenzung zu einer Funktionsübertragung findet sich bei Niedermeier/Schröcker, RDV 2001, 90, 93 sowie Wächter, CR 1991, 333 ff. Schaffland/Wiltfang, BDSG, § 3 BDSG Rn. 54a führen aus, dass Datenweitergabe im Rahmen des Outsourcing dann keine Übermittlung im Sinne des § 3 Abs. 4 Nr. 3 und Abs. 8 BDSG ist, wenn der Auftraggeber „Herr der Daten" bleibt, und der Auftragnehmer streng nach den Weisungen des Auftraggebers arbeiten muss. Übermittelt hingegen ein selbständiger Handelsvertreter aus seinen automatisiert verarbeiteten Datenbeständen Daten an die von ihm vertretenen Unternehmen, so handelt es sich um eine Übermittlung im Sinne des BDSG (siehe Schaffland/Wiltfang, BDSG, § 3 BDSG Rn. 53).

Endeffekt tatsächlich existierenden Verfügungsmacht über die Daten ab.[1643] So ist auch bei einer Auslagerung von Dienstleistungen auf ein Tochterunternehmen nicht automatisch eine *einwilligungsfreie* Auftragsdatenverarbeitung gegeben.[1644]
In den folgenden Ausführungen steht daher ebenfalls die Frage im Mittelpunkt, ob für die jeweilige Datenverarbeitung im Rahmen von Telearbeit eine Einwilligung des Betroffenen erforderlich sein könnte.
Hier kommt der bereits in der Einführung erwähnte Gedanke, dass es sich bei einem VPN um eine Konstruktion zu Lasten Dritter" handeln könnte, zum Tragen, wobei beantwortet werden muss, inwieweit „vertragszweckgemäß" Daten des Betroffenen durch ein VPN verarbeitet werden dürfen.[1645] So könnte ein VPN unter dem Aspekt, dass seitens eines Providers die „sichere Standortvernetzung" und ein „Arbeiten wie im Büro nebenan" angeboten wird,[1646] dazu führen kann, sämtliche für den Vertragszweck erforderlichen Daten ohne Einwilligung des Betroffenen und ohne Interessensabwägung an sämtlichen Standorten des VPN zu verarbeiten.. Dabei muss ebenso berücksichtigt werden, welche Möglichkeiten ein VPN-Auftraggeber hat, um den Datenschutz sowohl innerbetrieblich als auch außerbetrieblich – etwa im Rahmen der „heimischen" Telearbeit – sicherzustellen.

2. Zulässigkeit von Telearbeit

Die Frage nach der Zulässigkeit von Telearbeit und der damit verbundenen Verwendung von Daten Dritter ergibt sich nicht aus dem TKG oder TDDSG, sondern aus dem BDSG. So werden durch das Fernmeldegeheimnis gemäß § 88 TKG zwar auch der Inhalt der Kommunikation und damit nicht nur die Nutzer des Telekommunikationsdienstes, sondern gleichermaßen die Daten

[1643] Vgl. auch Fasbender, RDV 1994, 12, 14; Damann/Rabenhorst, CR 1998, 643, 643.
[1644] Vgl. hierzu Evers/Kiene, NJW 2003. 2726, 2728, die im Rahmen der Auslagerung von Finanzdienstleistungen diskutieren, ob § 11 BDSG Anwendung findet. Siehe hierzu außerdem Evers/Kiene, DB 2003, 2762, .
[1645] Siehe hierzu S. 7 sowie von Lewinski, NJW 2004, 349, 349, der wiederum auf Simitis in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 84 ff. verweist. Von Lewinski behandelt aber in dem Kontext „Vertrag zu Lasten Dritter" die Frage der Interessen von „Drittbetroffenen" und vermisst bei Simitis (aaO) die Auseinandersetzung mit der Frage, inwieweit bei der Datenverarbeitung durch Rechtsanwälte das Konzept des Vertrages zu Lasten Dritten vorliegt, da nach Ansicht von Simitis keine Abwägung mit den Interessen Drittbetroffener, etwa des Prozessgegners, stattfinden muss.
[1646] Siehe hierzu die Ausführungen in der Einführung S. 2.

Dritter bzw. anderer Betroffener geschützt.[1647] Aber die Frage, ob im Einzelfall die Benutzung der Inhaltsdaten zulässig ist, ergibt sich aus dem BDSG, [1648] da weder das TKG noch das TDDSG vorrangige Regelungen bezüglich des (verarbeiteten) Inhalts beinhalten.[1649]

Telearbeit, unabhängig davon ob in Form des Outsourcing oder des Arbeitens „von zu Hause", könnte daher gemäß der obigen Ausführungen einschränkend nur dann zulässig sein, sofern gemäß § 28 Abs. 1 Nr. 2 BDSG „kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt." Die nachfolgende Prüfung „berechtigte Interessen" unterteilt hierbei in die Datennutzung einerseits im häuslichen Bereich sowie andererseits in einem Betrieb (Zweigstelle, Tochterunternehmens).

a. Wahrung berechtigter Interessen

aa. Datennutzung im häuslichen Bereich

Ein berechtigtes Interesse gemäß § 28 Abs. 1 Nr. 2 BDSG kann wirtschaftlicher oder ideeller Natur sein.[1650] Daher ist die Telearbeit, insbesondere als Möglichkeit zur Kostenverringerung in einem Betrieb, als berechtigtes Interesse gemäß § 28 Abs. 1 Nr. 2 BDSG anzuerkennen.[1651]

Die Datenübertragung durch Telearbeit bzw. Datenweitergabe an die Telearbeiter im häuslichen Bereich sowie deren Kenntnisnahme der Daten fällt unter den Begriff des Nutzens gemäß § 3 Abs. 5 BDSG. Ein Nutzen der

---

[1647] Vgl. auch Büchner in: TKG- Kommentar (2. Auflage), § 85 TKG Rn. 1.

[1648] Zum Charakter des BDSG als Auffanggesetz siehe auch Schaffland/Wiltfang, BDSG, § 1 BDSG Rn. 37.

[1649] Siehe zur Übermittlung personenbezogener Daten als Inhalt eines Telefongesprächs oder einer E-Mail Däubler, Gläserne Belegschaften?, Rn. 334. Vgl. auch Gola/Schomerus, BDSG, § 10 BDSG Rn. 7. § 88 TKG schützt zwar den Inhalt der Kommunikation, dennoch kommt § 88 TKG hier nicht zur Anwendung, da in diesem Personenverhältnis kein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG vorliegt. Siehe zu „Inhaltsdaten" außerdem S. 105 und S. 347 („Inhaltsdaten" fallen unter das BDSG und nicht unter das TDDSG). Zu berücksichtigen ist, dass im Verhältnis von VPN-Auftraggeber und Dritten dies zweifelsfrei gelten muss, da der Dritte von vorneherein keinen Teledienst des VPN-Auftraggebers in Anspruch nimmt, sondern vielmehr ohne sein Zutun seine Daten verwendet werden.

[1650] Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 85.

[1651] Siehe Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 85. Dort werden unter anderem die Verbesserung des Betriebsergebnisses und die Verringerung der Kosten als berechtigte Interessen anerkannt. Vgl. zur Übertragung von Bankdienstleistungen auf dritte Unternehmen aus Gründen der Kostenminimierung Steding, BB 2001, 1693, 1699.

gespeicherten Daten liegt dann vor, wenn die Daten mit einer bestimmten Zweckbestimmung ausgewertet, zusammengestellt, abgerufen oder auch nur ansonsten zielgerichtet zur Kenntnis genommen werden sollen.[1652] Zu berücksichtigen ist, dass der Telearbeiter im Verhältnis zu seinem Arbeitgeber und aus Sicht des Betroffenen kein Dritter gemäß § 3 Abs. 8 BDSG ist, so dass der Tatbestand der Übermittlung nach § 3 Abs. 4 Nr. 3 BDSG nicht in Betracht kommt. Der (angestellte) Telearbeiter ist in den Betrieb eingebunden, und der Arbeitgeber ist und bleibt die für die Datenverarbeitung verantwortliche Stelle gemäß § 3 Abs. 7 BDSG,[1653] wobei Telearbeit im häuslichen Bereich des Arbeitnehmers aber auch keine Auftragsdatenverarbeitung gemäß § 11 BDSG darstellt.[1654] Zu berücksichtigen ist insbesondere, dass der Arbeitnehmer nicht allein dadurch zum Auftragnehmer wird, wenn er anstatt im Büro die gleiche Arbeit zu Hause erledigt. Es ergibt sich insoweit kein inhaltlicher Unterschied. Die Datenweitergabe innerhalb der verantwortlichen Stelle fällt damit lediglich unter den Begriff der Nutzung.[1655] Die Annahme eines „Nutzens" ist vorrangig (vor den Tatbeständen des Veränderns gemäß § 3 Abs. 4 Nr. 2 BDSG, des Sperrens gemäß § 3 Abs. 4 Nr. 4 BDSG oder des Löschens gemäß § 3 Abs. 3 Nr. 5 BDSG)[1656] ebenso aus dem Grunde gerechtfertigt, da der Informationsgehalt der Daten nicht zwangsläufig verändert wird.[1657] Bei Telearbeit steht vielmehr der zweckbestimmte Gebrauch der Daten im Vordergrund.[1658]

Für die Anwendbarkeit des § 3 Abs. 5 BDSG im Zusammenhang mit Telearbeit im häuslichen Bereich spricht außerdem der Vergleich zur Veröffentlichung von

[1652] Gola/Schomerus, BDSG, § 3 BDSG Rn. 42, die im Übrigen auf den Auffangcharakter der Regelung verweisen.
[1653] Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 8.
[1654] Gola/Jaspers, RDV 1998, 243, 245; Gola/Schomerus, BDSG, § 11 BDSG Rn. 10, die auf die arbeitsvertragliche Beziehung und die lediglich ausgelagert stattfindende Tätigkeit verweisen. Siehe auch Schaffland/Wiltfang, BDSG, § 11 BDSG Rn. 1a, die die Meinung vertreten, dass bei Telearbeit im heimischen Umfeld des Arbeitnehmers entweder Eigenverarbeitung oder Auftragsdatenverarbeitung in Betracht kommt. In diesem Sinne ebenso Walz in: Simitis, BDSG-Kommentar, § 11 BDSG Rn. 26. Vgl. außerdem Fischer/Schierbaum, CR 1998, S. 321, 324 sowie Boemke/Andersen, BB 2000, S. 1570, 1572.
[1655] Vgl. auch Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2. Rn. 70.
[1656] Ein Speichern kommt von vorneherein nicht in Betracht, da der Telearbeiter die Daten nicht erstmalig speichert, und die Speicherung zuvor bereits zum Zwecke ihrer weiteren Verwendung seitens des Arbeitgebers erfolgt ist.
[1657] Vgl. zum Begriff des Veränderns Gola/Schomerus, BDSG, § 3 BDSG Rn. 30. Siehe zum Verändern gemäß § 3 Abs. 4 S. 2 Nr. 2 BDSG ebenso Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2. Rn. 64.
[1658] Vgl. auch Gola/Schomerus, BDSG, § 3 BDSG Rn. 42.

Daten, die unter den Begriff des Nutzens fallen kann.[1659] Im Rahmen der Telearbeit erhalten Arbeitnehmer ebenso Zugriff auf Daten erhalten, die über das Internet veröffentlicht bzw. öffentlich zugänglich gemacht werden.[1660]

Da aber der Begriff „berechtigte Interessen“ als Anknüpfungspunkt einer nur ausnahmsweise zulässigen Verarbeitung angesehen wird,[1661] und von der Rechtsordnung gebilligt sein muss,[1662] muss zunächst die Abgrenzung zu § 28 Abs. 1 Nr. 1 BDSG vorgenommen werden. Dessen Anwendungsbereich ist grundsätzlich eröffnet, da seitens des (angestellten und dem Unternehmen zugehörigen) Telearbeiters insgesamt auf bereits erhobene[1663] Daten zugegriffen wird, deren Verarbeitung im unmittelbaren sachlichen Zusammenhang zwischen der beabsichtigen Verarbeitung und dem konkreten Vertragszweck zwischen VPN-Auftraggeber und Dritten steht:[1664] Der Telearbeiter greift auf Daten zu, die für die Erfüllung des Vertragsverhältnisses mit dem Dritten notwendig sind.[1665]

Fraglich ist, ob eine Datenverarbeitung nach § 28 Abs. 1 Nr. 1 BDSG auch im Rahmen der Telearbeit gerechtfertigt ist, da in § 28 Abs. 1 Nr. 1 BDSG das „Wie“ der Datenverarbeitung nicht geregelt ist. Man könnte somit zu der Annahme gelangen, dass Daten –auf jegliche Art und Weise -- im Verlauf ihrer Verarbeitung durch die speichernde Stelle genutzt werden dürfen, sofern etwa

[1659] Vgl. Gola/Schomerus, BDSG, § 3 BDSG Rn. 42, der darauf verweist, dass unter Nutzen gemäß
§ 3 Abs. 5 BDSG ebenso die Veröffentlichung fallen kann. Siehe auch Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 195, der das Bereithalten von Daten zum Abruf als Beispiel für das Nutzen nennt.

[1660] Wenn auch unter der Einschränkung von Zugriffsberechtigungen.

[1661] Vgl. Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 91.

[1662] Niedermeier/Schröcker, RDV 2001, 90, 94.

[1663] Die Erhebung von personenbezogenen Dritter im Rahmen eines Vertragsverhältnisses des Unternehmens bzw. VPN-Auftraggebers mit einem Dritten, etwa seinem Kunden oder einem Lieferanten, ist regelmäßig erforderlich, um Pflichten aus diesem Vertragsverhältnis mit dem Dritten zu erfüllen oder Rechte wahrzunehmen; vgl. auch Gola/Schomerus, BDSG, § 28 BDSG Rn. 13.

[1664] Vgl. Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 85; Auernhammer, BDSG, § 28 BDSG Rn. 12. Subjektive Erwartungen sind hierbei im Übrigen stets gleichgültig (vgl. Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 85). Siehe zum unmittelbaren sachlichen Zusammenhang ebenso Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 79.

[1665] Dies steht natürlich unter der Prämisse, dass Telearbeit im häuslichen Bereich des Arbeitnehmers die Arbeit im Betrieb ersetzt und der Telearbeiter mit den gleichen Daten in Berührung kommt, auf die er auch im Büro Zugriff hätte, um das Vertragsverhältnis mit dem Dritten zu erfüllen bzw. abzuwickeln.

deren erstmalige Erhebung und Speicherung zulässig sind, insbesondere zum Zwecke der Erfüllung des vertraglichen Verhältnisses erhoben worden sind.
Zu berücksichtigen ist aber folgendes: Aus § 28 Abs. 1 BDSG ergibt sich, dass sämtliche Merkmale („Erheben“, „Speichern“, „Verändern“, „Übermitteln“ und „Nutzen“) als Mittel für die Erfüllung eigener Geschäftszwecke nur dann zulässig sind, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient.[1666]
Dies bedeutet, dass unabhängig von der Zulässigkeit des erstmaligen Erhebens oder Speicherns „auch im Verlauf der Datenverarbeitung“ stets und auf den Einzelfall bezogen geprüft werden sollte, ob die jeweilige Nutzung, wie Telearbeit, der Zweckbestimmung des Vertragsverhältnisses dient und gerechtfertigt ist. So gibt es Verarbeitungsschranken.[1667] Der Zweck der vertraglichen Beziehung kann die interne Nutzung der Daten einschränken, und die Daten dürfen nicht innerhalb der verantwortlichen Stelle frei zirkulieren.[1668]
Diese Einschränkung ergibt sich gleichermaßen aus dem oben angestellten Vergleich zur Veröffentlichung. Auch diese kann eine Datennutzung darstellen und ist ebenso regelmäßig mit einer vorangehenden Datenerhebung und Datenspeicherung verbunden, die bereits auf ihre Zulässigkeit hin zu überprüfen waren. Dies gilt insbesondere, sofern bei Datenspeicherung die Veröffentlichungsabsicht noch gar nicht vorlag.[1669]
Des Weiteren ist zu berücksichtigen, dass der Betroffene nach § 35 Abs. 2 Nr. 1 BDSG die Löschung der Daten verlangen kann, wenn diese unrichtig sind. Diese können aber im Verlaufe der Datenverarbeitung unrichtig werden, etwa wenn der Sinngehalt durch eine Löschung des Kontextes verändert wird.[1670] In diesem Falle wird die Datenverarbeitung ebenso nachträglich unzulässig, so dass die Verarbeitungsstufe „Datenveränderung“ oder „Datenlöschung“ auf ihre Zulässigkeit hin zu überprüfen ist.

[1666] Siehe Gola/Schomerus, BDSG, § 28 BDSG Rn. 13, mit dem Hinweis, dass im Einklang mit der herrschenden Meinung ein „verarbeiten müssen“ zu fordern ist, auch wenn der Gesetzeswortlaut lediglich ein „dienen“ erfasst.
[1667] Siehe zu dem Begriff der Verarbeitungsschranken Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 106.
[1668] Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 115.
[1669] Vgl. Fn. 1659 und den Verweis unter anderem auf Gola/Schomerus, BDSG, § 3 BDSG Rn. 42.
[1670] Vgl. hierzu Gola/Schomerus, BDSG, § 35 BDSG Rn. 5.

Auch wenn darauf verwiesen wird, dass die Einbeziehung des Nutzens keine materielle Ausweitung des Gesetzes bedeute, sondern gewissermaßen allein der Output der Daten ist,[1671] ist damit noch nichts über die Zulässigkeit der einzelnen Verarbeitungsstufen gesagt.

Eine einmalige bzw. erstmalige zulässige Datenerhebung kann letztendlich keinen Freibrief für alle andere Verarbeitungsformen darstellen.

Der ursprüngliche Geschäftszweck, etwa die Durchführung und Abwicklung eines Vertragsverhältnisses, bleibt zwar bei Telearbeit im häuslichen Bereich erhalten, wenn die Datenerhebung für den konkreten Vertragszweck objektiv erforderlich war,[1672] die Verwendung ist jedoch nicht beliebig.

Sofern keine Bedingungen über die Verarbeitungsphasen vereinbart worden sind, wie es beispielsweise im Arbeitsverhältnis durch Vereinbarungen mit der Arbeitnehmervertretung möglich ist,[1673] muss zumindest das informationelle Selbstbestimmungsrecht beim Verwendungsprozess beachtet werden.[1674]

Dieses sollte nicht nur funktional im Sinne einer Personenbeschränkung,[1675] sondern ebenso an der Art und Weise der Verarbeitung ausgerichtet sein.

Im Sinne eines effektiven Datenschutzes ist daher stets die jeweilige Erhebung, jeweilige Verarbeitung und Nutzung im Einzelfall auf ihre Zulässigkeit geprüft werden.

Die jeweilige Verarbeitungsstufe[1676] muss demnach im Sinne eines Müssens[1677] dazu notwendig sein, das von den Parteien gemeinsam mit dem Vertrag verfolgte Ziel zu erreichen.[1678]

Ein „Muss“ des Unternehmers zur Telearbeit im häuslichen Bereich besteht jedoch nicht. Die Organisation des Betriebsablaufes liegt vielmehr in der freien Entscheidung des Arbeitgebers. Er könnte genauso gut die entsprechenden Arbeitsplätze in seiner betrieblichen Arbeitsstätte schaffen.

[1671] Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 2a und 2b, die im Übrigen die Datenerhebung als Input der Daten betrachten.

[1672] Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 91.

[1673] Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 106. Siehe im Übrigen Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 23zur Notwendigkeit einer Betriebsvereinbarung bei einer automatisierten Erfassung von Arbeitnehmerdaten.

[1674] Vgl. Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 115.

[1675] So Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 115.

[1676] Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 2b ordnen das Erheben der Daten als Vorstufe zum Speichern ein.

[1677] Siehe Gola/Schomerus, BDSG, § 28 BDSG Rn. 13.

[1678] Vgl. Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 85.

Die Existenz einer vertraglichen Bindung (im Sinne von § 28 Abs. 1 Nr. 1 BDSG) zwingt zwar zu einer restriktiven Anwendung der weiteren in § 28 BDSG geregelten Verarbeitungstatbestände (wie § 28 Abs. 1 Nr. 2, 3 BDSG), die daher eng ausgelegt werden müssen und nur ausnahmsweise zulässig sind.[1679]
Zu bedenken ist jedoch, dass in diesem Falle die Entscheidung für die Anwendbarkeit von § 28 Abs. 1 Nr. 2 BDSG und der Einbezug der Interessen des Betroffenen zu einem erhöhten Schutz des Betroffenen führt.
Wird die Zulässigkeit allein an § 28 Abs. 1 Nr. 1 BDSG gemessen, ist insgesamt noch nicht die Intensität der Verarbeitung mitberücksichtigt,[1680] die sich aus der Übersendung der Daten über das Internet verknüpft mit der Verarbeitung im heimischen Bereich ergibt.[1681] Auch wenn ebenso die Voraussetzungen des § 9 BDSG, insbesondere dessen Weitergabekontrolle gemäß Nr. 4 der Anlage zu § 9 BDSG,[1682] einzubeziehen sind, haben diese Vorgaben keine Relevanz für die Zulässigkeit der Datenverarbeitung.[1683]
§ 28 Abs. 1 Nr. 2 BDSG kann den Persönlichkeitsschutz des Betroffenen besser berücksichtigen

Diese Sichtweise entspricht im Übrigen ebenso der Forderung, bei der Konkretisierung der in § 28 BDSG enthaltenen Generalklauseln, sich zunächst und vor allem mit den möglichen Auswirkungen auf die informationelle Selbstbestimmung der Betroffenen auseinanderzusetzen und konsequenterweise stets der Interpretation den Vorzug zu geben, die der Situation der Betroffenen und ihren Belangen am ehesten Rechnung trägt.[1684]
Bei Telearbeit im häuslichen Bereich des Arbeitnehmers sollten daher die Verwendungsgrenzen berücksichtigt werden.

[1679] Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 78; Gola/Schomerus, BDSG, § 28 BDSG Rn. 9.
[1680] Vgl. zur Intensität der Verarbeitung Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 163.
[1681] Vgl. Wedde, DuD 1998, 576, 578; Wedde, NJW 1999, 527, 534; Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 11; siehe hierzu auch Zilkens/Werhahn, RDV 1999, 60, 63.
[1682] Siehe zur Weitergabekontrolle die Ausführungen von Schaffland/Wiltfang, BDSG, § 9 BDSG Rn. 112 ff.
[1683] Gola/Schomerus, BDSG, § 3a BDSG Rn. 2 verweisen darauf, dass § 9 BDSG ebenso wenig wie § 3a BDSG die Datenverarbeitung nicht notwendigerweise unzulässig machen.
[1684] Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 21.

Fraglich könnte in diesem Zusammenhang zwar sein, ob „Telearbeit an sich“ zu einem eigenen Geschäftszweck erhoben werden könnte, ohne diese Arbeitsform „lediglich“ als eine Art bzw. Unterfall der Nutzung nach § 28 Abs. 1 BDSG in Verbindung mit § 3 Abs. 5 BDSG einzustufen.
Dafür spricht, dass Datenverarbeitung durch Telearbeit gemäß § 28 Abs. 1 Nr. 1 BDSG als Mittel zum Zweck, d.h. zur Erreichung eines dahinter stehenden Geschäftszwecks, eines wirtschaftlichen Erfolgs, dient.[1685] So läge bei Schaffung von Arbeitsplätzen im heimischen Umfeld der Arbeitnehmer eine Datenverarbeitung vor, die als Hilfsmittel[1686] zur Erfüllung bestimmter anderer, eigener Zwecke der Daten verarbeitenden Stelle erfolgt,[1687] und zwar hier insbesondere die Verfolgung des Ziels zeitgemäßere Arbeitsbedingungen zu schaffen.
Zu berücksichtigen ist dennoch, dass die erstmalige Erhebung und Speicherung der relevanten Daten des Betroffenen im Rahmen eines Vertrags- oder sonstigen Vertrauensverhältnisses mit diesem stattfindet. In den seltensten Fällen wird eine Erhebung von Daten zum Zwecke der Durchführung von Telearbeit erfolgen. Sind die Daten einmal erhoben, so ändert sich durch ihre weitere Nutzung der ursprüngliche Geschäftszweck, etwa die Abwicklung eines Kaufvertrages, nicht. Außerdem reglementiert § 28 Abs. 1 BDSG die Datenverarbeitung als Mittel zum Zweck, ohne aber selbst das geschäftliche Interesse zu bilden.[1688]

Daher fällt Telearbeit insgesamt unter den Begriff der Nutzung gemäß § 3 Abs. 5 BDSG, stellt aber regelmäßig keinen eigenständigen Geschäftszweck dar, so dass sich die Zulässigkeit der Datennutzung „Telearbeit im häuslichen Bereich eines Arbeitnehmers“ nach den Anforderungen des § 28 Abs. 1 Nr. 2 BDSG richtet.[1689]

[1685] Gola/Schomerus, BDSG, § 28 BDSG Rn. 4.
[1686] Siehe zu diesem Begriff auch Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 3.
[1687] Vgl. hierzu auch Gola/Schomerus, BDSG, § 28 BDSG Rn. 4.
[1688] Gola/Schomerus, BDSG, § 28 BDSG Rn. 4.
[1689] Missverständlich ist im Übrigen, aus welchem Grunde Telearbeit erst dann zulässig sein soll, wenn keine anonymisierte oder pseudonymisierte Datenverarbeitung möglich ist (so Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 11). Denn die Vorgabe in § 3a BDSG, personenbezogene Daten möglichst in pseudonymisierter oder anonymisierter Form zu verarbeiten, trifft jegliche Datenverarbeitung und ist keine spezielle Zulässigkeitsvoraussetzung der Telearbeit. Im Übrigen können pseudonymisierte oder anonymisierte personenbezogene Daten, die auf dem Unternehmensrechner gespeichert sind,

Dementsprechend bzw. mangels eigenem Geschäftszweck ist der VPN-Auftraggeber gegenüber dem Betroffenen nicht verpflichtet ist, über den Einsatz von Telearbeitsplätzen nach § 4 Abs. 3 Nr. 2 BDSG aufzuklären bzw. zu informieren.[1690]

Insbesondere handelt es sich bei den Arbeitnehmern, die im eigenen häuslichen Bereich über einen Telearbeitsplatz verfügen, regelmäßig nicht um Dritte, sondern um die Mitarbeiter des Unternehmers, so dass sich hier von vorneherein nicht die Frage stellt, inwieweit der Betroffene mit der Übermittlung an Dritte gemäß § 4 Abs. 3 Nr. 3 BDSG rechnen musste.[1691]

Rechtspolitisch kann aber eine Aufklärung aus anderen Gründen wünschenswert sein. Laut § 4 Abs. 3 BDSG ist der Betroffene nur über die Tatsache der Erhebung zu informieren, und weder über den weiteren Inhalt, Anlass der Speicherung noch über die eingesetzten Sicherungsmethoden zu unterrichten.[1692] Dennoch kann diesbezüglich ein besonderes Aufklärungsbedürfnis des Betroffenen bestehen, und zwar vornehmlich bezüglich der Art und Weise der Übermittlung, welche Verschlüsselungsmethoden eingesetzt werden und ob überhaupt verschlüsselt wird. Das gesetzliche Auskunftsrecht nach § 34 BDSG erfasst im Übrigen nicht die äußeren Umstände der Nutzung der Daten.[1693]

Hierbei muss natürlich berücksichtigt werden, inwieweit der VPN-Auftraggeber zur Benachrichtigung über die eingesetzten Methoden verpflichtet ist, soweit hier eine Offenlegung seiner Geschäfts- und Betriebsgeheimnisse in Betracht kommt.[1694] Daher kann und muss eine Informationspflicht ausscheiden, sofern der Unternehmer verpflichtet wäre, die Absicherung seines Netzwerkes komplett offenzulegen, und sich damit unter Umständen Schaden zufügt, sofern

---

und auf welchen der Nutzer Zugriff erhalten soll, auch seitens des Telearbeiters in dieser pseudonymisierten oder anonymisierten Form bearbeitet werden.

[1690] Vgl. auch § 33 Abs. 1 BDSG; siehe hierzu Gola/Schomerus, BDSG, § 33 BDSG Rn. 7 sowie S. 110 ff. in dieser Arbeit zu den allgemeinen Unterrichtungspflichten.

[1691] Im Rahmen von § 4 Abs. 3 Nr. 3 BDSG und § 33 Abs. 1 S. 3 BDSG ist danach zu differenzieren, ob die Empfänger gemäß § 3 Abs. 8 BDSG Dritte sind; siehe Schaffland/Wiltfang, BDSG, § 4 BDSG Rn. 14 mit der Anmerkung, dass es sich um ein Redaktionsversehen handelt und mit Empfängern allein „Dritte“ gemeint sind, wie sich auch aus dem Wort „übermitteln“ ergebe. Zu der Frage, ob es sich bei den Telearbeitern, die im heimischen Umfeld tätig sind, um Auftragsdatenverarbeiter handelt, siehe oben S. 386.

[1692] Vgl. hierzu auch Schaffland/Wiltfang, BDSG, § 33 BDSG Rn. 5.

[1693] Siehe zum Auskunftsrecht gemäß § 34 BDSG Schaffland/Wiltfang, BDSG, § 34 BDSG Rn. 4 ff.

[1694] Siehe zu dem Begriff der Geschäfts- und Betriebsgeheimnisse S. 245 ff.

mögliche Angreifer nun in einfacher Form feststellen können, wo die technischen Schwachpunkte und Angriffsflächen liegen.
Dessen ungeachtet spricht aber nichts dagegen, den Vertragspartner als Betroffenen über die eingesetzten Sicherheitstechniken und Telearbeit zu informieren, beispielsweise bei Vertragsschluss. Denn sofern bei Massengeschäften nichts dagegen spricht, eine Einwilligung in die jeweilige Datenverarbeitung einzuholen,[1695] so kann noch weniger gegen eine Information oder Aufklärung bei Vertragsschluss sprechen.

bb. Outsourcing

Da Outsourcing[1696] ebenso wenig wie Telearbeit im häuslichen Bereich eines Arbeitnehmers im Sinne eines Muss erforderlich ist, kommt vorneherein der Anwendungsbereich des § 28 Abs. 1 Nr. 1 BDSG nicht in Betracht, sondern es muss vielmehr eine Interessenabwägung gemäß § 28 Abs. 1 Nr. 2 BDSG stattfinden.[1697] Das berechtigte Interesse zur Durchführung von Telearbeit kann auch hier in der Kostenverringerung liegen.[1698]

aaa. Auftragsdatenverarbeitung

Die bei der Erhebung, Verarbeitung oder Nutzung von Daten im Auftrag von Auftraggeber und Auftragnehmer zu beachtenden Verpflichtungen sind zwar durch § 11 festgeschrieben.[1699] Hierbei handeltes sich um eine innerbetriebliche Angelegenheit und Selbstkontrolle, die dem Aufgabenbereich des betrieblichen Datenschutzbeauftragten unterfällt und durch entsprechende Vertragsgestaltung zwischen Auftraggeber und Auftragnehmer sicher zu stellen

[1695] Vgl. Naujoks, in: Roßnagel, Handbuch Datenschutzrecht, 7.3 Rn. 40 ff.
[1696] Zum Begriff des Outsourcing siehe S. 382, insbesondere auch Fn. 1632. Im Übrigen ist hier nochmals darauf hinzuweisen, dass die Datenverarbeitung im Ausland vollständig von der rechtlichen Prüfung ausgeschlossen sein soll. Hierzu wird auf die bereits in der Einleitung dargestellten Ausführungen verwiesen (siehe S. 87 ff).
[1697] Festzustellen ist im Übrigen, dass durch diese Auffassung in die Entscheidungsfreiheit eines Unternehmers an einer arbeitsteiligen Wirtschaft nicht über Gebühr eingegriffen wird. Er kann sich weiterhin grundsätzlich externer Stellen bedienen, gegebenenfalls jedoch unter strengeren Zulässigkeitsvoraussetzungen.
[1698] Vgl. S. 385.
[1699] Gola/Schomerus, BDSG, § 11 BDSG Rn. 2. Anders als für die Zulässigkeit der Telearbeit im häuslichen Bereich des Arbeitnehmers gibt es hier also bereits eine den Datenschutz regelnde Vorschrift.

ist.[1700] Dementsprechend ist für die datenschutzrechtlichen Verpflichtungen im Verlaufe der Datenverarbeitung gegenüber dem Betroffenen klar, dass es nur ein „Entweder-Oder" geben kann.[1701]

Da aber § 11 BDSG die grundsätzliche Frage der Zulässigkeit der Datenweitergabe[1702] (an den Outsourcing-Partner) nicht regelt, kommt diesbezüglich die zusätzliche Anwendbarkeit von § 28 Abs. 1 Nr. 2 BDSG in Betracht.

Eine generelle Nichtanwendbarkeit von § 28 Abs. 1 Nr. 2 BDSG hätte zur Folge, dass die Handlung bzw. der Akt der Datenweitergabe (an sich) im Sinne eines Nutzens gemäß § 3 Abs. 5 BDSG[1703] an den Auftragsdatenverarbeiter nicht separat auf ihre Zulässigkeit hin geprüft werden würde, und der Betroffene selbst keine entsprechenden Korrekturrechte gemäß §§ 34, 35 BDSG in der Hand hätte. Nur bei zusätzlicher Einbeziehung der Voraussetzungen des § 28 Abs. 1 Nr. 2 BDSG werden die überwiegenden Interessen des Betroffenen bei der Datenweitergabe berücksichtigt. Hierauf kann auch nicht unter Berücksichtigung der Datenweitergabekontrolle gemäß Nr. 4 der Anlage zu § 9 BDSG verzichtet werden. Die Regelung schafft keinen gleichwertigen Interessensausgleich, da sie sich lediglich auf die technischen und organisatorischen Maßnahmen der Art und Weise des Datentransports bezieht.[1704] Die Frage, ob überhaupt die Einschaltung eines Auftragsdatenverarbeiters und Datenübertragung über das Internet gerechtfertigt ist, oder ob die Datenverarbeitung nicht im Betrieb selbst stattfinden kann, ist damit allerdings noch nicht geklärt.

Für die zusätzliche Anwendbarkeit von § 28 Abs. 1 Nr. 2 BDSG bezüglich des „Akt der Datenweitergabe" an den Auftragsdatenverarbeiter spricht auch, dass

[1700] Siehe hierzu auch Gola/Schomerus, BDSG, § 11 BDSG Rn. 22.

[1701] Vgl. auch Schaffland/Wiltfang, BDSG, § 27 BDSG Rn. 24 für die verbundenen Unternehmen.

[1702] Es wird hier bewusst der Begriff „Datenweitergabe" gewählt, da dem Begriff der „Datenübermittlung" eine Datenverarbeitung durch Dritte immanent ist, was jedoch bei einer Auftragsdatenverarbeitung nicht in Betracht kommt, da Auftragsdatenverarbeiter keine Dritten darstellen, Gola/Schomerus, BDSG, § 11 BDSG Rn. 3.

[1703] Hier müssen die obigen Überlegungen auf S. 385 ff. im Hinblick auf die Datennutzung entsprechend gelten, da auch Daten an Personen weitergegeben werden, die im Übrigen keine Dritten gemäß § 3 Abs. 8 BDSG darstellen. Vgl. auch Siehe Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2. Rn. 70, der auch bei einer Datenweitergabe zwischen der verantwortlichen Stelle und der im Auftrag tätigen Stelle eine Nutzung annimmt.

[1704] Vgl. zur Weitergabekontrolle die Ausführungen von Ernestus in: Simitis, BDSG-Kommentar, § 6 BDSG Rn. 110 ff.

die Regelungen des dritten Abschnitts den Schutz des Bürgers bei der Datenverarbeitung ergänzen sollen.[1705]

Zu berücksichtigen ist dennoch, dass § 11 BDSG gewissermaßen eine (Teil-) Sonderregelung für die Zulässigkeit der Datenweitergabe und eine Interessenabwägung beinhaltet, so dass die Erfüllung der Voraussetzungen durch Auftraggeber und Auftragnehmer schon per se dazu führt, dass die überwiegenden Interessen des Betroffenen, die es nach § 28 Abs. 1 Nr. 2 BDSG zu beachten gilt, zumindest teilweise erfüllt sind.

Sofern also die Voraussetzungen des § 11 BDSG vorliegen, insbesondere die sorgfältige Auswahl und schriftliche Auftragserteilung, ist die Datenweitergabe an den Dritten gemäß § 28 Abs. 1 Nr. 2 BDSG auch insoweit zulässig. Die Frage der Zulässigkeit der Datenweitergabe (übers Internet) an den Auftragsdatenverarbeiter kann allerdings noch von weiteren Faktoren, etwa von ausreichenden technischen und organisatorischen Maßnahmen, abhängen, wie im Folgenden gezeigt werden wird.

Unterrichtungspflichten gemäß § 4 Abs. 3 BDSG kommen auch bei der Auftragsdatenverarbeitung nicht in Betracht, da keine Daten übermittelt bzw. an Dritte weitergegeben werden.[1706] Eine Hinweis- bzw. Unterrichtungspflicht entfällt dementsprechend gemäß § 4 Abs. 3 Nr. 3 BDSG. Zu berücksichtigen ist außerdem, dass der Betroffene keine eigenen datenschutzrechtlichen Ansprüche gegen den Auftragsdatenverarbeiter, so dass er zur Wahrnehmung seiner Rechte nicht dessen Name benötigt. Lediglich im Hinblick auf die Art und Weise der Datenverarbeitung könnte sich in rechtspolitischer Hinsicht eine Unterrichtung empfehlen.

[1705] Schaffland/Wiltfang, BDSG, § 27 BDSG Rn. 1.

[1706] Auftragsdatenverarbeiter stellen keine Dritten im Sinne von § 3 Abs. 8 BDSG dar, siehe Gola/Schomerus, BDSG, § 11 BDSG Rn. 3. Siehe zum Ausschluss der Unterrichtungspflichten bereits die Ausführungen auf S. 392 ff.

bbb. Funktionsübertragung

Im Rahmen der Funktionsübertragung ist ebenso zu prüfen, inwieweit die Datenübermittlung nach § 28 Abs. 1 Nr. 2 BDSG zulässig ist.[1707] Aufgrund dessen, dass eine Funktionsübertragung an Dritte im Sinne von § 3 Abs. 8 BDSG, also an außerhalb der verantwortlichen Stelle stehende Personen,[1708] vorgenommen wird, liegt hier der Tatbestand der Übermittlung gemäß § 3 Abs. 4 Nr. 3 BDSG vor.
Anders als bei der Auftragsdatenverarbeitung gibt es bei der Funktionsübertragung keine dem § 11 BDSG entsprechende gesetzliche Regelung bezüglich datenschutzrechtlicher Anforderungen, so dass eine allgemeine Interessenabwägung gemäß § 28 Abs. 1 Nr. 2 BDSG im Hinblick auf die Datenübermittlung bzw. Datenweitergabe an den Dritten vorgenommen werden muss.[1709]

Im Hinblick auf etwaige Unterrichtungspflichten nach § 4 Abs. 3 BDSG ist zu berücksichtigen, dass nach einer Auffassung Outsourcing heutzutage ein gängiges Modell ist, so dass insgesamt keine Hinweis- oder Benachrichtigungspflichten in Frage kommen.[1710]
Eine solche Auffassung kann aber nur für Auftragsdatenverarbeiter und Telearbeiter, die ihren Arbeitsplatz im häuslichen Bereich eingerichtet haben, Geltung beanspruchen. Denn bei der Funktionsübertragung kommt insgesamt die Eigenschaft als Dritter nach § 3 Abs. 8 BDSG und damit die Hinweispflicht gemäß § 4 Abs. 3 BDSG in Betracht.[1711] Unerheblich ist im Übrigen, ob es sich bei den Dritten um Unternehmen innerhalb eines Konzerns handelt und/oder ob diese rechtlich selbständig sind oder nicht. Denn es kommt allein auf die konkrete und inhaltliche Ausgestaltung der Datenweitergabe an.

[1707] Vgl. Gola/Schomerus, BDSG, § 27 BDSG Rn. 5 zur Anwendbarkeit des § 28 Abs. 1 Nr. 2 BDSG im Rahmen der Auslagerung der Personaldatenverarbeitung sowohl für denjenigen, der die Funktion auslagert, als auch für denjenigen, der die Funktion wahrnimmt.
[1708] Vgl. hierzu auch Gola/Schomerus, BDSG, § 11 BDSG Rn. 9.
[1709] Siehe außerdem die Ausführungen von Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 56 ff. zur Datenübermittlung im Rahmen eines Vertragsverhältnisses.
[1710] Vgl. hierzu Gola/Schomerus, BDSG, § 4 BDSG Rn. 35.
[1711] Siehe auch Niedermeier/Schröcker, RDV 2001, 90, 94, die anhand des Beispiels eines Tochterunternehmens darstellen, dass das Tochterunternehmen sowohl Auftragdatenverarbeiter (und damit kein Dritter) sein kann, als auch eine Funktionsübertragung wahrnehmen kann.

Fraglich ist lediglich, ob eine Hinweispflicht auf die Kategorie von Empfängern ohne weitere Angaben über Name, Adresse, etc. gemäß § 4 Abs. 3 Nr. 3 BDSG erforderlich und ausreichend ist,[1712] oder darüber hinaus sogar spezifische Angaben über das jeweilige Unternehmen zu machen sind.[1713]
Zu berücksichtigen ist hierbei, dass mittlerweile die Auslegung und die Anforderungen an § 4 Abs. 3 BDSG durch die Datenschutzbehörden der einzelnen Bundesländer weiter gefasst worden sind.
So wird zwar danach unterschieden, ob es sich um ein Übermitteln gemäß § 3 Abs. 4 Nr. 3 BDSG, und damit um eine Datenweitergabe an Dritte, handelt.[1714] Aber gefordert wird eine konkrete Benennung der Adressaten, an welche Daten weitergegeben werden. Dazu ist die Aufführung von Name und Anschrift erforderlich, um dem Kunden die Möglichkeit zu geben, Auskunfts- und Löschungsersuchen unmittelbar an ihn zu richten.[1715] Die Benutzung von Gruppenbezeichnungen, wie etwa „inländische Tochterunternehmen“ ist unzulässig.[1716] Einschränkendes soll aus Praktikabilitätsgründen lediglich für Außendienstmitarbeiter gelten.[1717]

[1712] Im Zusammenhang mit Tochterunternehmen und der „Kategorie von Empfängern“ benennen Schaffland/Wiltfang, BDSG, § 4 BDSG Rn. 14 folgendes Beispiel: „Um sie umfassend beraten und betreuen zu können, möchten wir Ihnen auch die Leistungsangebote unserer Tochterunternehmen zukommen lassen.“
[1713] Siehe Gola/Schomerus, BDSG, § 4 BDSG Rn. 35, die eine solche spezifische Hinweispflicht über den Gesetzeswortlaut hinaus befürworten.
[1714] Siehe Schaffland/Wiltfang, BDSG, § 4a BDSG Anhang 1, wo im Rahmen der Einwilligungserklärung für die Datenübermittlung zwischen einer Bank und ihren Kooperationspartnern (auch Außendienstmitarbeiten) von Daten<u>übermittlung</u> ausgegangen wird, so dass sich insoweit darauf schließen lässt, dass damit eine Funktionsübertragung, also eine Datenweitergabe an Dritte gemeint ist. Siehe auch Schaffland/Wiltfang, BDSG, § 4a BDSG Anhang 1 unter Anmerkung Nr. 1; dort wird im Rahmen der Einwilligungserklärung des Kunden darauf Bezug genommen, dass Daten an dritte Unternehmen, auch innerhalb eines Konzerns, nur mit Einwilligung des Kunden weitergegeben werden dürfen. Eine Einwilligung des Kunden nach § 4 BDSG (und nicht nur eine Interessenabwägung) ist in diesem Zusammenhang „Bank/Kooperationspartner und Betreuung der Kunden“ im Übrigen aus dem Grunde wichtig, da die Datenweitergabe hier nicht durch § 28 BDSG gedeckt ist. Denn insoweit ist das Bankgeheimnis betroffen, so dass eine Einwilligung erforderlich ist. § 28 BDSG kommt nur zur Anwendung, wenn nicht vorrangig eine Einwilligung nach § 4 Abs. 1 BDSG erforderlich ist. Da nach § 1 Abs. 3 S. 2 BDSG die Verpflichtung zur Wahrung Geheimhaltungspflichten unberührt bleibt, wozu auch das Bankgeheimnis zählt (vgl. Gola/Schomerus, BDSG, § 1 BDSG Rn. 25 und § 28 BDSG Rn. 11; Simitis in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 126; a.A. Schaffland/Wiltfang, BDSG, § 1 BDSG Rn. 35), ist bei der Datenübermittlung einer Bank an Kooperationspartner im Sinne von Dritten stets eine Einwilligung erforderlich (siehe Schaffland/Wiltfang, BDSG, § 3 BDSG Rn. 55 zu der Frage der Zugänglichmachung von Daten, die dem Bankgeheimnis unterliegen, an Dritte und einem damit verbundenen Verstoß gegen das Bankgeheimnis).
[1715] Siehe Schaffland/Wiltfang, BDSG, § 4a BDSG Anhang 1 unter Anmerkung Nr. 3.
[1716] Siehe Schaffland/Wiltfang, BDSG, § 4a BDSG Anhang 1 unter Anmerkung Nr. 3.
[1717] Siehe Schaffland/Wiltfang, BDSG, § 4a BDSG Anhang 1 unter Anmerkung Nr. 3.

Im Sinne eines ausreichenden Datenschutzniveaus ist die letzte Auffassung allerdings als Ausnahme zu begreifen.
So ist es zumutbar, sofern der VPN-Auftraggeber nach § 4 Abs. 3 Nr. 3 BDSG verpflichtet ist, seinem Kunden (dem Betroffenen) den Namen und die Adresse seiner externen Lieferanten (Nutzer des VPN) zu nennen, sofern diese Zugriff auf Kundendaten erhalten, insbesondere im Zusammenhang mit der Ausführung der Lieferung.

cc. Besondere rechtliche Erwägungen zur Zulässigkeit

Obgleich bei der Telearbeit keine vollständige Zweckänderung[1718] im Sinne von § 28 Abs. 2 BDSG erfolgt, da die Daten nach wie vor im Rahmen des „ursprünglichen“ Vertragsverhältnisses zwischen VPN-Auftraggeber und Dritten verwendet werden, sollte die Art und Weise der Nutzung auch die Interessen des Betroffenen ausreichend berücksichtigen.[1719]
Diese Einbeziehung der Interessen des Betroffenen kann am besten erfüllt werden, sofern der Anwendungsbereich des § 28 Abs. 1 Nr. 2 BDSG eröffnet wird, vor allem da in die Rechte des Betroffenen nicht stärker eingedrungen werden sollte, als es der Zweck des Vertragsverhältnisses erfordert.[1720] Denn sofern keine Zweckänderung erfolgt, dürfen personenbezogene Daten innerhalb der verantwortlichen Stelle nur verwendet werden, wenn und soweit dies erforderlich ist.[1721]

Im Übrigen lässt das informationelle Selbstbestimmungsrecht, das seine Grundlage in Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG findet, und dem Betroffenen das Recht gewährt, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen,[1722] eine Datenverarbeitung ohne oder gegen dessen Willen oder ob und inwieweit Dritte über seine Daten verfügen, nicht

[1718] Siehe zur Zweckbestimmung eines Vertragsverhältnisses auch Gola/Schomerus, BDSG, § 28 BDSG Rn. 13 ff.
[1719] Siehe auch Wedde, DuD 1998, 576, 579 zur Anwendbarkeit von § 28 BDSG, sofern Telearbeitsplätze eingerichtet werden.
[1720] Siehe zu dieser These für das Arbeitverhältnis insbesondere BAG, RDV 1987, 129, 131.
[1721] Vgl. Globig in: Roßnagel, Handbuch Datenschutzrecht, 4.7 Rn. 95.
[1722] BVerfGE 65, 1, 48.

zu.[1723] Daher kann im Einzelfall auch das „inwieweit“ der Datenverarbeitung entscheidend sein.

Problematisch könnte zwar sein, ob diese Fragestellung überhaupt im Privatrechtsverkehr Berücksichtigung finden sollte, da zum einen Privatrechtssubjekte generell untereinander in rechtlicher Hinsicht keinen Zwang über die Art und Weise der Ausübung des informationellen Selbstbestimmungsrechts ausüben können.[1724] Bezieht man zum anderen in diese Überlegung die These mit ein, dass die informationelle Selbstbestimmung nicht als Herrschaftsmacht über die personenbezogenen Daten verstanden und als eigentumsähnliche Ausschluss- und Verfügungsmacht ausgestaltet werden dürfe,[1725] so könnten Zweifel daran auftauchen, dass der Betroffene ein generelles Mitspracherecht bei der Verarbeitung seiner Daten. Dies gilt insbesondere bezüglich der Art und Weise der Datenverarbeitung, sofern die erstmalige Datenerhebung und Datenspeicherung bereits gemäß § 4 Abs. 1 BDSG zulässig war. Wird zudem unterstellt, dass die Stelle über die Daten verfügungsberechtigt ist, die sie erhoben hat,[1726] dann könnte dementsprechend die „einmalige“ Legitimation nach § 28 Abs. 1 Nr. 1 BDSG ausreichen, um die Zulässigkeit von Telearbeit zu begründen, ohne diese nochmals einer Interessenabwägung zu unterwerfen.[1727]

Nichtsdestotrotz ist Ziel des Modernisierungsgutachtens, Datenschutz zu fördern, zu effektiveren und risikoadäquat zu gestalten.[1728] Dies bedeutet auch, dass eine (unterstellte) mangelnde Verfügungsmacht seitens des Betroffenen

---

[1723] Geiger, NVwZ 1989, 35, 36.

[1724] Kilian, CR 2002, 921, 925.

[1725] Siehe hierzu das Modernisierungsgutachten, S. 37.

[1726] Siehe ebenso das Modernisierungsgutachten, S. 37.

[1727] Sofern man die Daten des Dritten bzw. Betroffenen gleichermaßen als personenbezogene Daten desjenigen betrachtet, der sie verarbeitet (etwa weil sie ihn im Sinne von § 3 BDSG ebenso bestimmbar machen), oder als dessen Betriebs- und Geschäftsgeheimnisse (vgl. § 17 UWG), dann geht man konform mit der Aussage des Modernisierungsgutachtens, dass Modelle der Wirklichkeit in der Regel soziale Beziehungen abbilden, die beide Partner betreffen und nicht nur einer Person zugeordnet werden können (Modernisierungsgutachten, S. 37 Fn. 55). Denn so können Kundendaten sowohl Betriebs- und Geschäftsgeheimnisse bzw. - soweit es sich bei dem VPN-Auftraggeber um eine natürliche Person handelt- personenbezogene Daten des VPN-Auftraggebers, als auch (selbstverständlich) personenbezogene Daten des Betroffenen selbst darstellen. Unabhängig von der Frage, ob damit ebenso zwangsläufig verbunden, dem Betroffenen die Herrschafts- und Verfügungsmacht über seine Daten in Abrede zu stellen (siehe hierzu im Besonderen Kilian, CR 20002, 921, 923 ff., der dieser These kritisch gegenübersteht und argumentativ entgegentritt), ist es gerechtfertigt, Datenschutz möglichst effektiv zu gestalten; siehe hierzu auch die folgende Ausführung.

[1728] Vgl. Modernisierungsgutachten, S. 34, wo außerdem neben Effektivität und Risikoadäquanz die Forderung nach mehr Verständlichkeit und höherer Attraktivität des Datenschutzes aufgestellt wird.

über seine Daten nicht dazu führen kann, den Datenschutz dort einzuschränken, wo wirksame und effektive gesetzliche Regelungen bestehen, den Datenschutz sicher(er) zu gestalten, so insbesondere durch eine Interessenabwägung gemäß § 28 Abs. 1 Nr. 2 BDSG im Rahmen der Zulässigkeitsprüfung von Telearbeit.

Insoweit sind die Aussagen des BVerfG, die gemäß § 1 Abs. 1 BDSG als Regelungsziel des Datenschutzes festgelegt sind, [1729] eindeutig: Das Grundrecht auf informationelle Selbstbestimmung gewährleistet „die Befugnis des Einzelnen grundsätzlich selbst über die Preisgabe und die Verwendung seiner persönlichen Daten zu bestimmen".[1730] Dies stellt kein Recht des Verarbeiters dar, auch wenn es für diesen unverständlich sein kann, dass ihm zwar die Programme auf einem Rechner gehören sollen, aber nicht die unter Umständen mit viel Mühe beschafften damit verarbeiteten personenbezogenen Daten.[1731]

Des Weiteren spricht ebenso eine Gegenüberstellung von § 9 BDSG und § 28 BDSG für die Anwendbarkeit des § 28 Abs. 1 Nr. 2 BDSG. Die Vorschrift des § 28 BDSG befindet sich im ersten Unterabschnitt des dritten Abschnitts des BDSG unter „Rechtsgrundlagen der Datenverarbeitung". Hier sind die Voraussetzungen enthalten, die eine Datenverarbeitung im Einzelfall unzulässig machen können und die dem Betroffenen eigene Mitspracherechte und Korrekturrechte bezüglich seiner Datenverarbeitung gewähren.[1732]

Die Sicherstellung von organisatorischen und technischen Maßnahmen gemäß § 9 BDSG hingegen unterliegt zunächst einmal der innerbetrieblichen Selbstkontrolle.[1733] Zwar kontrollieren die zuständigen Aufsichtsbehörden der Länder die Ausführung des BDSG und können nach § 38 Abs. 5 BDSG die Beseitigung festgestellter technischer oder organisatorischer Mängel verlangen.[1734]

[1729] In § 1 Abs. 1 BDSG ist das Ziel normiert, das Vorrecht des Betroffenen zu garantieren, so dass dieser selbst darüber entscheiden kann, wer unter welchen Umständen und für welchen Zweck auf seine Daten zugreifen darf (vgl. hierzu Simitis in: Simitis, BDSG-Kommentar, § 1 BDSG RN. 25, der darauf verweist, dass sich trotz anders lautendem Wortlaut dieser Anknüpfungspunkt an das informationelle Selbstbestimmungsrecht des Betroffenen im Sinne der Bundesverfassungsgerichtsentscheidung durchgesetzt hat).

[1730] BVerfG, NJW 1984, 419, 422.

[1731] Vgl. hierzu Weichert, NJW 2001, 1463, 1467.

[1732] Vgl. auch Gola/Schomerus, BDSG, § 35 BDSG Rn. 1.

[1733] Vgl. auch Gola/Schomerus, BDSG, § 9 BDSG Rn. 2 ff.

[1734] Siehe zu den Weisungs- und Eingriffsrechten im Einzelnen Schaffland/Wiltfang, BDSG, § 38 BDSG Rn. 26 ff.

Jedoch gewährt die Anwendung von § 28 Abs. 1 Nr. 2 BDSG im Hinblick auf die Zulässigkeit der Datenerhebung und Datenverarbeitung dem Betroffenen das Recht, von vorneherein eine Datenerhebung und Verarbeitung zu verhindern sowie bei Unzulässigkeit der Speicherung nachträglich eine Löschung der Daten gemäß § 35 Abs. 2 Nr. 1 BDSG zu verlangen, während bei § 28 Abs. 1 Nr. 1 BDSG, ohne Berücksichtigung des „Wie“ und auf die ursprüngliche Datenverarbeitung bezogen, die Datenverarbeitung zunächst grundsätzlich zulässig ist[1735] und erst in einem zweiten Schritt zu prüfen wäre, ob die verarbeitende Stelle überhaupt die erforderlichen organisatorischen und technischen Maßnahmen nach § 9 BDSG sicher stellt.

Dies macht ebenfalls wegen der Strafvorschriften einen erheblichen Unterschied, da nach §§ 43 Abs. 2 Nr. 1, 44 BDSG das unbefugte Verarbeiten von Daten eine Ordnungswidrigkeit darstellt und unter Umständen strafbar ist. Die Rechtswidrigkeit ergibt sich hierbei aus den Erlaubnistatbeständen des BDSG für die Verarbeitung, wie beispielweise § 4 Abs. 1 BDSG oder §§ 28 ff. BDSG.[1736] Ist bereits die Nutzungsform „Telearbeit“ durch § 28 Abs. 1 Nr. 1 BDSG gedeckt, so besteht für den VPN-Auftraggeber kein „Druck“ auf sämtliche technische oder organisatorische Maßnahmen im besonderen Maße zu achten. Ist aber Telearbeit bzw. der Akt der Datenweitergabe stets nur unter den Voraussetzungen des § 28 Abs. 1 Nr. 2 BDSG zulässig, so ist Telearbeit dann unzulässig und damit im Sinne von §§ 43 Abs. 1 Nr. 2, 44 BDSG unbefugt bzw. rechtswidrig[1737], sofern die Interessenabwägung zu Lasten des Betroffenen ausfällt.
Dies gilt zumindest im Zusammenhang mit Outsourcing, da hier Daten an Dritte übermittelt werden und dies eine Datenverarbeitung gemäß § 3 Abs. 4 Nr. 3 BDSG darstellt, welche gemäß §§ 43 Abs. 2 Nr. 1, 44 StGB im Falle mangelnder Befugnis strafbar sein kann. § 43 Abs. 1 Nr. 2 BDSG stuft zwar das unbefugte Nutzen der Daten nicht als ordnungswidriges Verhalten ein, so dass

[1735] Niedermeier/Schröcker, RDV 2001, 90, 97 verweisen etwa darauf, dass das berechtigte Interesse der verarbeitenden Stelle im Rahmen der Zweckbestimmung kraft Gesetzes überwiegt und § 28 Abs. 1 Nr. 1 BDSG damit lex specialis zu § 28 Abs. 1 Nr. 2 BDSG ist.
[1736] Vgl. Gola/Schomerus, BDSG, § 43 BDSG Rn. 26; Schaffland/Wiltfang, BDSG, § 43 BDSG Rn. 36 ff.
[1737] Siehe auch Gola/Schomerus, BDSG, § 43 BDSG Rn. 26, die anmerken, dass die Tatbestandsmäßigkeit die Rechtswidrigkeit indiziert und dies durch den Begriff „unbefugt“ zum Ausdruck gebracht wird.

bei Telearbeit im Wege der Auftragsdatenverarbeitung oder im häuslichen Bereich des Arbeitnehmers insoweit keine Bußgeldvorschriften oder Strafvorschriften in Betracht kommen.[1738] Letztendlich spricht hier aber für die Anwendbarkeit des § 28 Abs. 1 BDSG der Vergleich zur Funktionsübertragung, die stets an § 28 Abs. 1 S. 1 BDSG zu messen ist.
Einer Funktionsübertragung ist die mangelnde Kontrollmöglichkeit über die anschließende Datenverarbeitung immanent. Ein Defizit an Kontrolle, welches durch besondere Zulässigkeitsvoraussetzungen ausgeglichen werden kann, ist aber ebenso bei Telearbeit im häuslichen Bereich und Auftragsdatenverarbeitung zu bejahen, sofern von der speichernden Stelle Daten zur Einsicht oder zum Abruf über das Internet bereitgehalten werden, wobei darüber hinaus die Defizite im heimischen Umfeld zu berücksichtigen sind.

Telearbeit, unabhängig davon ob Telearbeitsplatz im häuslichen Bereich oder Outsourcing, ist daher einschränkend nur dann zulässig, sofern im Sinne von § 28 Abs. 1 Nr. 2 BDSG „kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt."

[1738] Gola/Schomerus, BDSG, § 43 BDSG Rn. 20. Die Frage ist allerdings, ob man hier nicht ebenso ein redaktionelles Versehen unterstellen kann, da letztendlich der Begriff des Nutzens gemäß § 3 Abs. 5 BDSG keine materielle Ausweitung des Gesetzes bedeutet (Schaffland/Wiltfang, BDSG, § 28 BDSG Rn. 2a), sondern allein einen Auffangtatbestand (Gola/Schomerus, BDSG, § 3 BDSG Rn. 42), so dass es als unbillig erscheint, gerade für den Betroffenen relevante Handlungen wie unbefugte Veröffentlichungen (vgl. Gola/Schomerus, BDSG, § 3 BDSG Rn. 42) als nicht ordnungswidriges oder strafbares Verhalten einzustufen. Daher sollte im Einzelfall ebenso die unbefugte Heimtelearbeit als Ordnungswidrigkeit gemäß § 43 Abs. 2 Nr. 1 BDSG geahndet werden können (siehe andererseits aber auch Gola/Schomerus, BDSG, § 43 BDSG Rn. 20 mit der Vermutung, dass die Nutzung bewusst nicht einbezogen worden ist, weil die Nutzungsformen zu vielfältig sind).

b. Entgegenstehende Interessen des Betroffenen

Als entgegenstehendes Interesse des Dritten im Sinne eines Betroffenen kommt der Schutz seiner personenbezogenen Daten in Betracht.
Das BDSG unterscheidet zwischen allgemeinen personenbezogenen Daten und besonderen Arten personenbezogener Daten, die es zu schützen gilt. Letztere werden gemäß § 3 Abs. 9 BDSG geschützt und auch als sensitive oder sensible Daten bezeichnet.[1739]
Bei diesen sensitiven oder sensiblen Daten handelt es sich um Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.
Aber auch nicht sensitive Daten, wie Name, Adresse, Alter, etc. des Betroffenen sind bei einer Interessenabwägung zu berücksichtigen.

c. Interessenabwägung

Die Abwägung zwischen den Interessen des VPN-Auftraggebers bzw. Arbeitgebers und dem Betroffenen wird in den nachfolgenden Ausführungen als eigenständiger Punkt behandelt.[1740] Dies beruht darauf, dass derjenigen Auffassung nicht gefolgt nicht wird, die ein berechtigtes Interesse nur annimmt, sofern es hierfür keine zumutbare Alternative gibt.[1741] Es ist insgesamt vorteilhafter, die berechtigten Interessen losgelöst von der ebenfalls nach § 28 Abs. 1 Nr. 2 BDSG erforderlichen Interessenabwägung zu betrachten, und deren Vorliegen bei jedem tatsächlichen Interesse wirtschaftlicher oder ideeller Natur zu bejahen.[1742] Denn im Rahmen dieser Interessenabwägung wird geprüft, inwieweit ein schutzwürdiges Interesse des Betroffenen an dem

[1739] Schladebach, CR 2003, 225, 226; Simitis, NJW 1998, 2473, 2477 (sensitive Daten); Däubler, NZA 2001, 874, 877 (sensible Daten). Vgl. außerdem Däubler, NZA 2001, 874, 877.
[1740] Siehe auch Büllesbach, CR 2000, 11, 14, der auf die Erforderlichkeit der Interessenabwägung Bezug nimmt.
[1741] Gola/Schomerus, BDSG, § 28 BDSG Rn. 34.
[1742] Siehe auch Niedermeier/Schröcker, RDV 2001, 90, 95 für den Bereich der Auslagerung des Marketings an ein Tochterunternehmen.

Ausschluss der Verarbeitung überwiegt, wobei dies nur anhand der individuellen Situation beantwortet werden kann.[1743]
Sofern anderenfalls bereits bei der Prüfung der berechtigten Interessen die Möglichkeit einer zumutbaren Alternative untersucht wird, würde bereits im Vorfeld eine Interessenabwägung vorgenommen, die in diesem Falle zu der Frage führt, ob es dem jeweiligen Unternehmer zumutbar ist, mehr Arbeitsplätze in seinen Räumlichkeiten zu schaffen anstatt sich für die Einrichtung von Telearbeit zu entscheiden. Diese Fragestellung ist jedoch aufgrund der heutigen Situation und der Globalisierung nicht zielführend, so dass vielmehr entscheidend sein sollte, auf welche Art und Weise sich Datenschutz im Wege der Telearbeit sinnvoll umsetzen lässt. Allerdings ist stets für den Einzelfall unter Abwägung der Interessen zu prüfen ist, ob und welche Daten im Wege der Telearbeit verarbeitet werden dürfen, oder ob Telearbeit vollständig zu unterbleiben hat.
Demgemäß ist bezogen auf die jeweiligen[1744] zu verarbeitenden Daten zu prüfen, ob der VPN-Auftraggeber bzw. Unternehmer ein berechtigtes Interesse an ihrer Verarbeitung mittels Telearbeit hat, wobei bei der Frage der Erforderlichkeit der Datenverarbeitung nur zugrunde gelegt werden sollte, ob ein Verzicht hierauf (für den Unternehmer) nicht sinnvoll wäre, ohne aber den strengen Maßstab der Zumutbarkeit anzulegen.[1745]

Ein **zusätzliches** Problem ergibt sich außerdem aufgrund des Exklusivitätsverhältnisses des TKG und TDDSG zum BDSG.[1746] Erfolgt hier eine strenge Anwendung dieses Exklusivitätsgrundsatzes, würde eine nicht zu rechtfertigende Ungleichbehandlung zwischen VPN-Auftraggebern der „Offline-Welt" zu VPN-Auftraggebern der „Online-Welt" vorliegen. Denn so wäre letzteren – bei gleicher Interessenlage - jegliche Telearbeit und Funktionsübertragung versagt, da Kundendaten bzw. die Bestandsdaten des Kunden gemäß § 5 TDDSG und § 95 Abs. 3 TKG stets nur mit Einwilligung des

[1743] Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 98. Der Widerstreit der Interessen ist über eine am konkreten Verarbeitungsprozess orientierte Abwägung zu lösen (Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 97). Bei der Prüfung des berechtigten Interesses kann eine Auswahl bezüglich der zu verwendenden Daten (siehe hierzu Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 94) nicht unabhängig von den Interessen des Betroffenen getroffen werden.
[1744] Vgl. Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 94.
[1745] Vgl. aber Gola/Schomerus, BDSG, § 28 BDSG Rn. 34.
[1746] Siehe S. 92.

Kunden verarbeitet dürften.[1747] Etwas anderes gilt gemäß diesen Regelungen nur, wenn die jeweilige Verarbeitung für das Vertragsverhältnis unbedingt erforderlich wäre. Eine solche zwingende Notwendigkeit wurde bereits abgelehnt.[1748]

Dementsprechend wäre von vorneherein eine Abwägung zwischen den Interessen des VPN-Auftraggebers und des Betroffenen unter Berücksichtigung des § 28 BDSG ausgeschlossen. Dies ist jedoch weder angemessen noch zielführend, da im Hinblick auf Telearbeitsverhältnisse weder von Telekommunikationsunternehmen noch von Teledienstanbietern größere datenschutzrechtliche Gefahren ausgehen als von Unternehmen der „Offline-Welt". Lediglich im Hinblick auf Werbezwecke oder Zwecke der bedarfsgerechten Diensterbringung kann einschränkend argumentiert werden, dass es aufgrund der „Verknüpfungsmöglichkeiten im Internet" datenschutzgerechter ist, eine ausdrückliche Einwilligung des Kunden einzufordern. So enthielt insbesondere § 5 Abs. 2 TDDSG a.F. eine Klarstellung, dass die Verarbeitung und Nutzung der Bestandsdaten für Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste nur zulässig ist, soweit der Nutzer in diese ausdrücklich eingewilligt hat. Dadurch wurde die Anwendung des § 28 BDSG gerade ausgeschlossen. Im Rahmen der Telearbeit muss hingegen insgesamt die identische Interessenlage der Unternehmen und der Betroffenen berücksichtigt werden, die keine unterschiedliche rechtliche Behandlung rechtfertigt und erforderlich macht.

[1747] Siehe zum grundsätzlichen Einwilligungserfordernis gemäß § 4a BDSG bei Telekommunikationsdiensten Gramlich in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 89 TKG(1998), Band 1, Rn. 115 sowie Gramlich in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 94 TKG(2004), Band 2, Rn. 9.

[1748] Siehe die Ausführungen zu § 28 Abs. 1 Nr. 1 BDSG auf S. 387 ff.

aa. Datennutzung im häuslichen Bereich

Bei der Frage, ob die am Verhältnismäßigkeitsgrundsatz ausgerichtete Abwägung keinen Grund zur Annahme bietet, dass die Speicherung der in Frage stehenden Daten zu dem damit verfolgten Zweck schutzwürdige Belange des Dritten bzw. Betroffenen beeinträchtigt,[1749] kommt es im Wesentlichen darauf an, wie der Datenschutz seitens des VPN-Auftraggebers im Zusammenhang mit den Telearbeitsplätzen im häuslichen Bereich des Arbeitnehmers gewährleistet wird.

Der VPN-Auftraggeber hat im Sinne von § 9 BDSG sämtliche erforderlichen technischen und organisatorischen Maßnahmen zu treffen.[1750] Insgesamt ist die Interessenabwägung am konkreten Verarbeitungsprozess vorzunehmen,[1751] wobei hierbei auf die informationelle Selbstbestimmung des Betroffenen abgestellt wird.[1752] Ein wichtiges Instrument zur Sicherstellung der erforderlichen technischen und organisatorischen Maßnahmen stellt der Arbeitsvertrag dar, in welchem diese Fragen eingehend geregelt und der Telearbeiter zur Einhaltung bestehender datenschutzrechtlicher Vorschriften sowie zur Geheimhaltung verpflichtet werden kann.[1753]

Wenn der Datenverarbeitungsprozess jedoch hohe Sicherheitsmaßnahmen beinhaltet, die dem betrieblichen Datenschutz nahezu ebenbürtig sind, so können keine überwiegenden Interessen des Betroffenen gegen eine Verarbeitung sprechen.[1754]

[1749] Vgl. auch BGH, NJW 1986, 2505, 2505 zur Zulässigkeit der Speicherung von Daten und Beeinträchtigung von schutzwürdigen Belangen.
[1750] Siehe zu Zugriffsrechten und Zugriffsschutz sowie § 9 BDSG auch Geis, Recht im eCommerce, S. 70 ff.
[1751] Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 97.
[1752] Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 98.
[1753] Siehe Albrecht, NZA 1996, 1240, 1243.
[1754] Siehe hierzu Wedde, Telearbeit, S. 133 mit dem Hinweis, dass der Arbeitgeber für die Einhaltung der gesetzlichen Vorgaben allein verantwortlich ist und sich von dieser Verantwortung nicht durch entsprechende Vereinbarungen mit den Beschäftigten freimachen kann. Vgl. außerdem Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 79 mit dem Hinweis, dass bei ausgelagerter Datenverarbeitung der Arbeitgeber die Verantwortung dafür trägt, dass die erforderliche Datensicherheit auf dem im Betrieb üblichen Niveau weiterhin gewährleistet bleibt.

aaa. Technische Maßnahmen

Zu den technischen Maßnahmen gehören gemäß der Anlage zu § 9 BDSG die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Weitergabekontrolle sowie das Trennungsgebot.[1755] Eine voll

Diese Sicherheit im technischen Bereich kann vor allem dadurch erreicht werden, dass ein Datenzugriff stets nur von den Telearbeitsplätzen ausgehend auf die mittels eines Gateway geschützte Unternehmenszentrale oder einen anderen mittels Gateway gesicherten Standort stattfinden darf und niemals umgekehrt stattfinden. Dies hängt damit zusammen, dass auf dem Gateway die Tunnel terminiert und die Sicherheitseinstellungen und die Benutzerverwaltung konfiguriert werden. Hier sind insbesondere die Parameter für die Authentifizierung der Nutzer, die auf Daten des Unternehmens-Server bzw. Intranets zugreifen wollen, sowie gegebenenfalls der Datenverschlüsselung festgelegt.[1756]

Bei einem Software-VPN ist allerdings fraglich, inwieweit ein Schutz erzielt werden kann, der dem Schutz eines Gateway-VPN ebenbürtig ist.[1757]

Darüber hinaus ist zu berücksichtigen, dass es selbst bei einem Gateway-VPN verschiedene Schutzmöglichkeiten und auch Authentifizierungsverfahren gibt. So ist es nicht nur möglich, die Gateways einem besonderen Zertifizierungsverfahren zu unterziehen,[1758] sondern es können darüber hinaus unterschiedliche Authentifizierungsverfahren in Betracht kommen.[1759] Eine Authentifizierung dient zwar in erster Linie dazu, unberechtigte Zugriffe auf das Firmennetz zu verhindern, hat aber damit gleichermaßen Schutzfunktion bezüglich personenbezogener Daten der Betroffen. Denn durch eine gute und

[1755] Schlachter in: Noack/Spindler, Unternehmensrecht und Internet. S. 215. Siehe zu diesen Begriffen nebst näherer Erläuterung auch Basisinformation Telearbeit des Projekts „Online-Forum Telearbeit“, S. 18.
[1756] Siehe oben S. 46 ff.. Vgl. außerdem zu IPSec: Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 31.
[1757] Vgl. hierzu auch die Ausführungen auf S. 235 ff. sowie die Hinweise in Fn. 227.
[1758] Siehe das Angebot von T-Online „SecureVPN-Benutzerhandbuch“, S. 20 ff., insbesondere S. 23, sowie die obigen Ausführungen auf S. 235.
[1759] Dies sind Sachverhalte, über welche der Provider den VPN-Auftraggeber aufklären müsste, sofern er das Systemmanagement des VPN oder Gateway erbringt. Ist allerdings der VPN-Auftraggeber der Betreiber des Gateways, so muss er sich selbständig um die entsprechenden Maßnahmen kümmern (vgl. hierzu die Ausführungen auf S. 234 ff.).

sichere Authentifizierung von Nutzern kann ebenso verhindert werden, dass auf die Daten des Betroffenen durch unbefugte Personen Zugriff genommen wird. Diese Ausführungen zu den unterschiedlichen technischen Möglichkeiten im Hinblick auf die Realisierung eines VPN stellen aber nicht die einzigen Themen dar, die ein VPN-Auftraggeber zu beachten hat. So gibt es bei den VPN-Protokollen ebenfalls mehrere technische Möglichkeiten.[1760]

IPSec gilt zurzeit als das beste Sicherheitsprotokoll.[1761] Daher ist fraglich, ob dieses Protokoll nicht stets bei Telearbeitsplätzen verpflichtend einzusetzen ist.[1762] Denn zu berücksichtigen ist, dass dieses Protokoll nicht nur Datenverschlüsselung sondern auch ein Schlüsselmanagement bietet, so dass dadurch ebenso der Betroffene besser geschützt wird, da dadurch unberechtigte Zugriffe auf seine Daten erschwert werden.[1763] Auch wenn kryptographische Verfahren bestehen und als gut befunden werden,[1764] sollte dennoch bei der Übertragung von personenbezogenen Daten im Internet darauf geachtet werden, dass die Daten desjenigen, der diese Übertragung nicht selbst veranlasst hat, bestmöglich durch erweiterte technische Schutzmöglichkeiten gesichert sind. Es werden zwar Empfehlungen zur Stärke der Verschlüsselung bzw. zur Schlüssellänge abgegeben.[1765] Es darf aber ebenso wenig die Datenintegrität und Authentifizierungsmöglichkeiten außer Acht gelassen werden. Ein VPN wird nicht nur durch den Einsatz von Datenverschlüsselungen sicher, sondern ebenso durch zusätzliche Maßnahmen, die sicherstellen, dass die Daten während ihrer Übertragung nicht verändert werden können und ein Dritter nicht die Möglichkeit hat, sich als der wahre Absender oder legitimierte und zugriffsberechtigte Nutzer des VPN auszugeben.[1766]

[1760] Siehe S. 35 ff., und insbesondere den Hinweis auf die unterschiedlichen Kombinationsmöglichkeiten von mehreren Protokollen, z.B. „IPSec mit L2TP“ (Fn. 256).
[1761] Siehe oben S. 39 ff. und den Hinweis auf L2Sec als Verschlüsselungsprotokoll, was – zumindest von dem Anbieter T-Online – als gleichwertig eingestuft wird.
[1762] Siehe zu IPSec oben S. 39 ff. mit dem Hinweis, dass andere Sicherheitsprotokolle erhebliche Schutzlücken aufweisen. Auch die IETF (siehe zur IETF S. 28 Fn. 100) hat empfohlen, den Tunnelverkehr mittels IPSec zu verschlüsseln (Böhmer, Virtual Private Networks, S. 213 in der 1. Auflage – vgl. nun die Ausführungen in der 2. Auflage auf S. 227).
[1763] Siehe zur Datenverschlüsselung und zum Schlüsselmanagement S. 40.
[1764] Siehe hierzu etwa die Vorschläge Hinweise im IT-Grundschutz-Katalog, Sicherheit in der Informationstechnik, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik, Loseblattsammlung, Stand 2005, abrufbar unter www.bsi.de.
[1765] 32. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten Teil 18.6.3.
[1766] 32. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten Teil 18.6.3.

Gerade wenn bekannt ist, dass ein Unternehmen seinen Nutzern, wie Arbeitnehmern oder Tochterunternehmen, Telearbeit und ein VPN anbietet, kann dieses Netz gezielten Angriffen ausgesetzt sein, so dass generell keine nur zufällige Kenntnisnahme Dritter in Betracht kommen kann.[1767] Daher reicht es im Einzelfall nicht aus, lediglich die Daten zu verschlüsseln, sondern es muss darüber hinaus für deren Integrität und Authentizität Sorge getragen werden.[1768] So sollte auch sichergestellt sein, dass die Datenschlüssel ständig wechseln.[1769] Diese Merkmale bietet beispielsweise IPSec.[1770] Insbesondere ist diesbezüglich zu beachten, dass ein VPN einerseits nicht bereits per se den Datenschutz sicherstellen kann, [1771] und dass IPSec andererseits zu den gängigen technischen Verfahren zählt, wie den aktuellen Produktbeschreibungen zu entnehmen ist.[1772] Durch entsprechend einfach und verständlich gehaltene Bedienungshandbücher wird dem jeweiligen Nutzer eine einfache Handhabung ermöglicht.[1773]

Da sich die Technik stets fortentwickelt, ist es jedoch eine Frage des Einzelfalls, ob nicht darüber hinaus auch andere IPSec gleichwertige Verschlüsselungsmethoden bei einem VPN existieren.[1774] Denn aufgrund der sich ändernden Bedingungen sollten keine absoluten technischen Sicherheitsmaßnahmen definiert werden, sondern vielmehr eine abstrakte Orientierung an den Datenschutzzielen erfolgen.[1775]

[1767] Vgl. aber den 32. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten Teil 18.6.3., in dem eine 40 bis 55 Bit-Verschlüsselung empfohlen wird, wenn ein gezielter Angriff unwahrscheinlich ist.

[1768] Vgl: die Ausführungen im 32. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten Teil 18.6.5, in denen darauf hingewiesen wird, dass Ansatzpunkte für Angriffe auf Verschlüsselungen weniger in unzureichenden Schlüssellängen zu suchen sind, als in Schwächen des Algorithmus und bei der Implementierung.

[1769] Lienemann, Virtuelle Private Netzwerke, S. 81.

[1770] Lienemann, Virtuelle Private Netzwerke, S. 81.

[1771] In diesem Sinne aber der 32. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten Teil 18.6.8.

[1772] Siehe hierzu S. 40.

[1773] Vgl. das Angebot von T-Online „directVPN Administrator-Benutzerhandbuch“. Auf S. 3 wird im Übrigen auf die Verwendung von IPSec verwiesen.

[1774] Insbesondere ist auch zu beachten, ob IPSec, was stets nur in der Lage ist IP-Datenpakete zu tunneln, im Einzelfall überhaupt einsetzbar ist, oder ob nicht auch eine Kombination unterschiedlicher Sicherheitsprotokolle in Betracht kommt (L2TP mit IPSec), siehe hierzu die Verweise in Fn. 1760. Siehe hierzu auch das Angebot von T-Online „SecureVPN-Benutzerhandbuch“ zum Sicherheitsprotokoll L2Sec, S. 208/209 sowie S. 74 (zu „IPSec over L2Sec“).

[1775] Vgl. zu sicheren Kommunikationsverbindungen auch die Ausführungen von Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 28 ff. Außerdem verweist Jacob, DuD 2000, 5, 10 darauf, dass technischer Datenschutz nicht primär an den technischen Komponenten festgemacht werden sollte, sondern es sollte sich vielmehr an den Schutzdimensionen der Daten orientiert werden. Siehe auch die Ausführungen von Engel-

Auf jeden Fall sollte dieses oder aber ein in nachvollziehbarer Weise vergleichbares Protokoll als Mindeststandard für die Zulässigkeit der Verarbeitung personenbezogener Daten im Rahmen der Telearbeit gefordert werden. [1776] Nur dann wird tatsächlich der Zustand eines „privaten" Netzes geschaffen, der ein Arbeiten wie im Büro nebenan ermöglicht. Dies gilt insbesondere unter dem Aspekt, dass bei einem Unternehmen, welches bekanntermaßen Telearbeit durchführt, gezielte Angriffe auf das Netz gerade nicht unwahrscheinlich sind.

Zu beachten ist bei der Wahl des Protokolls vor allem, dass einige Provider[1777] bei Telearbeitsplätzen im häuslichen Bereich nicht in der Lage sind, IPSec anzubieten, da seitens der von Ihnen angebotenen IPSec-Implementierung nicht die Zuweisung von dynamischen IP-Adressen unterstützt wird.[1778] Folge wäre, dass jeder Telearbeitsplatz im häuslichen Bereich des Arbeitnehmers eine statische IP-Adresse benötigen würde, was aufgrund der Knappheit der weltweiten IP-Adressen ein grundsätzliches Problem darstellt.[1779]
Hier müsste Telearbeit im heimischen Umfeld des Arbeitnehmers dann unterbleiben, sofern es keine gleichwertigen Verschlüsselungsmethoden gibt. Dies sind für den VPN-Auftraggeber wesentliche Fragestellungen, die regelmäßig nur mittels eines auf den Einzelfall bezogenen Beratungsgesprächs zwischen Provider und VPN-Auftraggeber abklärbar sind. Zu berücksichtigen ist jedoch, dass der Provider nicht zwangsläufig gemäß § 109 Abs. 1 TKG zur Information und entsprechenden Schutzmaßnahmen verpflichtet ist, sondern

---

Flechsig, DuD 1997, 8, 14, und den dort enthaltenen Hinweis, dass bestimmte technische Verfahren im Hinblick auf zukünftige technische Entwicklungen nicht vorgeschrieben werden.

[1776] Siehe Böhmer, Virtual Private Networks (2. Auflage), S. 229 mit dem Hinweis, dass zwar darauf verwiesen wird, dass es derzeit keine Alternative zu IPSec gebe (und es besser sei als PPTP und L2TP), aber dass dieses Protokoll dennoch nicht ganz kritiklos gesehen werde. Siehe ebenso die Ausführungen in der Computerwoche vom 21.01.2006 (http://whitepaper.computerwoche.de/index.cfm?pid=1&fk=61&pk=466) mit dem Hinweis, dass sich seit geraumer Zeit Zeitschriftenbeiträge über IPSec häufen. In diesen Artikeln sei immer wieder die Rede davon, dass IPSec der höchste Sicherheits-Standard und das für jede Netzwerk-Topologie uneingeschränkt einsetzbare VPN-Protokoll sei. Die Autoren möchten in ihrem Beitrag jedoch zeigen, dass IPSec nur in ganz bestimmten Umgebungen ohne zusätzliche Erweiterungen eingesetzt werden kann.

[1777] Siehe das Angebot von T-Online „SecureVPN-Benutzerhandbuch", S. 217.

[1778] Siehe hierzu aber auch Lipp, VPN, S. 177, der darauf verweist, dass dieses Problem dadurch gelöst werden kann, sofern bei der Auswahl der IPSec-Client-Implementierung darauf geachtet wird, dass diese eine dynamische Zuweisung der offiziellen IP-Adressen unterstützen.

[1779] Dies gilt zumindest zum momentanen Zeitpunkt, da zukünftig ein neues Protokoll dafür Sorge tragen soll, dass weltweit mehr IP-Adressen zur Verfügung stehen (siehe hierzu anstatt vieler Davis, IPSec, S. 28, der das so genannte IPv6-Datagrammformat darstellt, welches das IPv4-Datagrammformat ablösen soll).

nur, sofern er in seinem räumlichen Einflussbereich das Management des Gateways übernimmt.[1780] Hier zeigt sich wiederum, dass für die Beurteilung des Datenschutzes eines Online-Dienstes die Betrachtung des Mehrpersonenverhältnisses wichtig ist. Daher muss sich der VPN-Auftraggeber gegebenenfalls selbständig um die technischen Möglichkeiten und Alternativen bemühen und entsprechend kundig machen.

Die einzelnen zu treffenden Maßnahmen hängen im besonderen Maße von dem Umfang der geplanten Datenverarbeitung ab. So steht bei einigen Tunneling-Protokollen wie L2TP im Vordergrund, nicht auf dem Internet-Protokoll IP basierende Protokolle über das Internet zu transportieren.[1781] Das Thema „Datensicherheit" wird aber bei diesen Protokollen nachrangig behandelt wird. Der VPN-Auftraggeber kann sich daher überlegen, ob er solche Protokolle verwendet, um seine eigenen unternehmensbezogenen Daten, die keine Daten Dritter betreffen, über das Internet zu übertragen. Aber bei einem VPN, bei welchem gleichfalls personenbezogene Daten Dritter übertragen werden sollen, ergibt die Interessenabwägung, dass stets Verschlüsselungsprotokolle zu verwenden sind.[1782] Denn zu beachten ist, dass mittlerweile Verschlüsselungsmaßnahmen zum Stand der Technik gehören.[1783]

[1780] Vgl. die Ausführungen auf S. 250 ff.

[1781] So etwa das so genannte Layer-2-Tunneling-Protokoll (L2TP), vgl. Lipp, VPN, S. 172. Siehe hierzu in diese Arbeit auch S. 35 ff.

[1782] Die Gateways sind für die Sicherheitsstrategie des Tunneling-Verfahrens verantwortlich. Dies ist die entscheidende Stelle, auf welchem die Tunnel terminiert werden und die Sicherheitseinstellungen und die Benutzerverwaltung konfiguriert werden. Hier sind insbesondere die Parameter für die Authentifizierung der Nutzer, die auf Daten des Servers des Unternehmens bzw. Intranets zugreifen wollen, sowie gegebenenfalls der Datenverschlüsselung festgelegt. Hier arbeiten sämtliche Dienste zum Verpacken und Entpacken der Netzwerkprotokolle, der Datenkomprimierung, der Authentifizierung und der Kontrolle der Verbindungsqualität (vgl. oben S. 46 ff. sowie Lipp, VPN, S. 289). Allein auf einem Rechner des einzelnen Nutzers kann diese Sicherheitsstrategie des Tunneling-Verfahrens nicht implementiert werden (auf dem einzelnen Rechner wird je nach Tunneling-Protokoll allenfalls eine Software installiert, die der Sicherheitsstrategie in dem Gateway entspricht, vgl. Lipp, VPN, S. 406/ 407).

[1783] Koenig/Röder, CR 2000, 667, 671, die die SSL-Verschlüsselung ansprechen.

Daher kann insgesamt eine Pflicht zur Verschlüsselung auch bejaht werden,[1784] da das Schutzbedürfnis des Betroffenen überwiegt, sofern seine personenbezogenen Daten ohne sein Wissen im Internet versendet werden. Es kann vor allem nicht zu Lasten des Betroffenen gehen, sofern sich ein Unternehmer zu einer Datenverarbeitung „per Internet“ entschließt. Dann muss aber der bestmögliche Schutz des Betroffenen, der keinen unmittelbaren Einfluss auf die Datenverarbeitung nehmen kann, erreicht werden. Dies ergibt sich ebenso aus Nr. 3 der Anlage zu § 9 BDSG, der voraussetzt, dass kein unbefugter Zugriff auf die Daten erfolgen darf und Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.[1785]
Daraus folgt, nicht nur bei „reinen“ Software-VPN (die also keine zusätzlichen Gateways aufweisen) im Einzelfall genau zu überlegen, inwieweit diese den Schutz der personenbezogenen tatsächlich umfassend sicherstellen können[1786]
Es ist darüber hinaus ebenso zu untersuchen, inwieweit bei der Datenübertragung die zusätzlichen technischen Möglichkeiten der Datenintegrität und Authentifizierung, wie sie beispielsweise IPSec bietet, einzusetzen sind.
Außerdem muss im Falle von sensitiven bzw. sensiblen[1787] Daten ebenso geprüft werden, ob deren Verarbeitung im Rahmen von Telearbeitsplätzen (im häuslichen Bereich des Arbeitnehmers) nicht vollständig, und zwar auch beim

---

[1784] Zu der Pflicht zur Verschlüsselung von E-Mail-Kommunikation siehe Backu, ITRB 2003, S. 251 ff. (insbesondere auch S. 253). Backu (aaO) führt aus, dass es sich zum einen bei §§ 28, 29 BDSG um Schutzgesetze im Sinne von § 823 Abs. 2 BGB handelt. Zum anderen legen auch die Maßnahmen nach § 9 BDSG (siehe etwa Nr. 4 der Anlage zu § 9 BDSG) nahe, dass eine Pflicht besteht, sensible Daten bei ihrer Übermittlung zu schützen (Backu aaO). Siehe zur Pflicht zur Verschlüsselung bei Telekommunikationsdiensten und dem Stand der Technik Koenig/Röder, CR 2000, 667 ff. Vgl. außerdem Fickert/Nau/Gerling, DuD 2003, 223, 225, die zwar nicht von einer rechtlichen Verpflichtung, aber davon ausgehen, dass es in vernetzten Umgebungen, und zwar bereits in lokalen Netzwerken, allgemein üblich sei, Daten zentral abzulegen, und dass in diesem Zusammenhang auch der Anspruch erhoben wird, die Daten während der Übertragung gegen unbefugte Einsichtsnahme und Manipulation zu sichern. Röhrborn/Katko, CR 2002, 882, 887 nehmen außerdem zur Frage einer Verschlüsselungspflicht von W-Lan-Netzen Stellung und normieren eine Pflicht der Anbieter, ihre ungeschützten Zugänge durch Aufrüstung der Sicherheitsmaßnahmen zu schützen, insbesondere da entsprechende Verschlüsselungsprotokolle bereits entwickelt worden seien. Siehe zu den zivilrechtlichen Pflichten eines Webhost-Providers etwa Cichon, Internetverträge (1. Auflage), S. 70, dessen Nebenpflicht zum Schutz der gespeicherten Daten die Herstellung von Firewall-Systemen sei. Dies bedeutet, dass auch in zivilrechtlicher Pflicht eine Pflicht dazu besteht, die Daten der Kunden gegen fremde Angriffe zu sichern.
[1785] Siehe hierzu ebenso Gola/Schomerus, BDSG, § 9 BDSG Rn. 25.
[1786] Siehe zu den Voraussetzungen eines Software-VPN S. 53 ff., zu den Nachteilen insbesondere Fn. 227. Denn zu berücksichtigen ist, dass der Zugriffsschutz gegenüber einem mittels Gateway gesicherten VPN schwächer sein kann.
[1787] Siehe zu den sensiblen bzw. sensitiven Daten S. 403.

Einsatz von Verschlüsselungsprotokollen wie IPSec und dem Einsatz von Gateways, zu unterbleiben hat.[1788]

Die Forderung, dass hinsichtlich sensitiver Daten Telearbeit im heimischen Umfeld des Arbeitnehmers zu unterbleiben hat,[1789] ist auf die Unsicherheit im heimischen Bereich zurückzuführen. Sofern jedoch im Zusammenhang mit sensitiven Daten eine bestmögliche Datenverschlüsselung[1790] sowie autorisierter Datenzugriff eingesetzt wird und darüber hinaus sichergestellt ist, dass der im häuslichen Umfeld tätige Telearbeiter die Möglichkeit hat, die Daten –ohne diese notwendigerweise auf seinem eigenen Rechner speichern zu müssen - auf dem Server des Unternehmers im Wege eines Application Service Providing zu bearbeiten,[1791] dann kann unter diesem Aspekt über die Zulässigkeit der Verarbeitung sensitiver Daten nachgedacht werden.[1792] Die Unsicherheit im heimischen Bereich wäre somit begrenzt auf das Risiko einer möglichen Einsichtnahme in die Daten durch Dritte, etwa sofern ein Mitbewohner dem Telearbeiter bei der Datenverarbeitung „über die Schulter schaut".

Hier wäre aber zu überlegen, ob dieses Risiko durch eine entsprechende Verpflichtungserklärung des Telearbeiters, Dritten keine Einsicht in die Daten zu gewähren, behoben werden könnte. Insbesondere kann eine solche Situation der unbefugten Einsichtnahme gleichermaßen im Betrieb auftreten, beispielsweise wenn ein Vertriebsmitarbeiter einem Mitarbeiter aus der Personalabteilung auf den Bildschirm schaut – was natürlich durch entsprechende Anweisungen an die Mitarbeiter auch nicht möglich sein sollte, aber dennoch nicht ausgeschlossen ist. Zumindest ist die Frage erlaubt, ob in solchen Fällen weiterhin die berechtigten Interessen des Betroffenen einer Verarbeitung vollständig entgegenstehen.

[1788] Siehe hierzu die nachfolgenden Ausführungen auf S. 421 ff.

[1789] Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 11.

[1790] Vgl. zu den Verschlüsselungsmöglichkeiten oben S. 39 ff. sowie zur Empfehlung der IETF Fn. 1082.

[1791] Zur Möglichkeit des Application Service Providing siehe oben S. 74 und Fn. 356.

[1792] Vgl. auch Zilkens/Werhahn, RDV 1999, 60, 63, die die Ansicht vertreten, dass nicht generell die Verarbeitung sensibler personenbezogener Daten verboten werden sollte, sondern dass für jeden Einzelfall die konkreten Bedingungen am Arbeitsplatz an der Sensibilität der zu verarbeiteten Daten zu messen und danach zu entscheiden, ob eine Verarbeitung im Rahmen der Telearbeit vertretbar ist. So könne im Rahmen einer Risikoanalyse berücksichtigt werden, ob dem Telearbeitenden ein eigenes, abschließbares Arbeitszimmer zur Verfügung steht oder nicht.

Zwar bleibt die Netzunsicherheit des Internets grundsätzlich bestehen, da es absolut sichere Verschlüsselung niemals geben wird,[1793] aber diese absolute Sicherheit kann in keinem Betrieb sichergestellt werden, da auch hier grundsätzlich die Möglichkeit besteht, Türen zu Serverräumen aufzubrechen.[1794] Die Frage ist daher, ob die Gefahr der unbefugten Einsichtnahme aufgrund der heutigen Verschlüsselungsmöglichkeiten im Internet nicht derart minimiert ist, dass damit eine Situation geschaffen ist, die tatsächlich einem Arbeiten „wie im Büro nebenan" gleichkommt. Insbesondere, sofern seitens des VPN-Auftraggebers allein die Möglichkeit geschaffen wird, die Daten auf dem Server des Unternehmens zu bearbeiten, ohne diese auf den eigenen Rechner downloaden zu können.
Eine Antwort auf diese Frage kann jedoch nicht losgelöst von den notwendigen organisatorischen Maßnahmen und den überwiegenden Interessen des Betroffenen im Einzelfall gefunden werden, wie sich aus den folgenden Ausführungen ergibt.

bbb. Organisatorische Maßnahmen

(1) Instruktionen seitens des Arbeitgebers

Zu den organisatorischen Maßnahmen gehören die Verschwiegenheitsverpflichtung[1795] des Arbeitnehmers und die Pflicht, Unbefugten den Zutritt zu seinem heimischen Arbeitsplatz bzw. Rechner zu verweigern.[1796] Die letztgenannten Verpflichtung ist in der praktischen Umsetzung allerdings Schwierigkeiten ausgesetzt, da der Zutritt Dritter im

[1793] Hanau/Hoeren/Andres, Private Internetnutzung durch Arbeitnehmer, S. 18.
[1794] Siehe Barta, Datenschutz im Krankenhaus, S. 131 ff. zu den Sicherheitsanforderungen, die an einen Krankenhausbetrieb erwartet werden. So ist dort unter Punkt 1 die „Zugangskontrolle" genannt und die damit verbundene Gewährleistung, dass Unbefugten der Zugang zu den Datenverarbeitungsanlagen verwehrt ist, sowie unter Punkt 5 die „Zugriffskontrolle", die sicherstellen soll, dass allein Berechtigte auf die Daten zugreifen können. Diese Sicherheitsmaßnahmen können jedoch ebenso wenig eine absolute Sicherheit gewähren, auch wenn sie lokal bzw. innerhalb des Krankenhauses ohne Einsatz von Datenübertragung per Internet durchgeführt werden.
[1795] Siehe zur Verschwiegenheitsverpflichtung der Arbeitnehmer gemäß § 5 BDSG Wedde, Telearbeit, S. 130 mit dem Hinweis, dass diese auch nach Beendigung des Arbeitsverhältnisses fortbesteht.
[1796] Schlachter in: Noack/Spindler, Unternehmensrecht und Internet. S. 215; siehe auch Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 26.

häuslichen Bereich nicht ausgeschlossen werden kann.[1797] Hier könnte allenfalls der Arbeitgeber (unter entsprechender Kostenerstattung)[1798] die ausschließliche Verwendung eines abschließbaren Raumes für betriebliche Zwecke verlangen. Dies ist jedoch eher als Ausnahme anzusehen.

Außerdem sind seitens des Arbeitgebers geeignete, d.h. verschließbare und stabile Aufbewahrungsmöglichkeiten sowie Transportbehälter (für den Transport von Daten zwischen Telearbeitsplatz und Arbeitsstelle) zur Verfügung zu stellen.[1799] Diese verschließbaren Transportbehälter werden bei der Datenübertragung im Internet durch die oben beschriebenen Verschlüsselungstechniken, insbesondere IPSec, ersetzt, welche in der Lage sind, dass Datenpaket vollständig in ein anderes IP-Datenpaket einzupacken.[1800]
Fernerhin muss der Arbeitgeber nicht nur klare Vorgaben dahingehend erteilen, welche Daten gespeichert werden können und welche Daten unverzüglich zu löschen sind,[1801] sondern die strikte Trennung zwischen Privatbereich und betrieblichem Bereich in der Weise verlangen, dass es nicht zu einer Vermengung der privaten und betrieblichen Daten auf dem Rechner des Nutzers kommt.[1802] Eine solche Trennung ließe sich optimal ermöglichen, sofern der Telearbeiter nur die Möglichkeit hätte, auf dem Unternehmensserver die Daten zu bearbeiten und zu speichern, ohne diese aber auf seinen heimischen Rechner herunterzuladen, so wie Application Service Providing die Möglichkeit bietet. Eine weitere Möglichkeit wäre, dass der Arbeitgeber dem Arbeitnehmer (unter entsprechender Übernahme der Kosten) einen weiteren (Arbeits)Rechner zur Verfügung stellt. [1803]

[1797] Vgl. hierzu die Ausführungen von Wedde, Telearbeit, S. 128 unter zusätzlichem Bezug auf das Arbeiten in Hotelzimmern und im ICE.
[1798] Siehe Wedde, Telearbeit, S. 86 ff. zur Kostenerstattungspflicht des Arbeitgebers in Arbeitsverhältnissen (§ 670 BGB) sowie speziell für Telearbeit Rn. 367 ff.
[1799] Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 27.
[1800] Siehe hierzu S. 42.
[1801] Siehe auch Geis, Recht im eCommerce, S. 70 ff. (insbesondere S. 71 bis S. 73) mit dem Hinweis, dass auch der Betriebsrat einen Online-Zugriff auf Personaldaten erhalten kann, aber ebenso nur unter Einhaltung eines ausreichenden Schutzniveaus.
[1802] Siehe zu dem Verbot der Nutzung privater Rechner Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 22. Bei Gola/Schomerus, BDSG § 9 BDSG Rn. 22, die den Datenschutzbericht aus dem Jahre 1999 der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen (S. 130) zitieren, in welchem sich außerdem eine Auflistung von Regelungen findet, die im Zusammenhang mit Datenschutz bei Telearbeit zu beachten sind.
[1803] Siehe zur Kostentragungspflicht des Arbeitgebers Wedde Fn. 1798.

(2) Kontrollrechte des Arbeitgebers

Ein Arbeitgeber muss außerdem im Rahmen seiner organisatorischen Maßnahmen das Recht haben, den Datenschutz im heimischen Bereich kontrollieren zu können, da er letztendlich die verantwortliche Stelle für den Datenschutz darstellt.[1804]

Ebenso sind nach § 38 Abs. 4 BDSG die mit der Datenschutzkontrolle beauftragten Personen berechtigt, soweit es erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume zu betreten und dort Prüfungen und Besichtigungen vorzunehmen.

Diese Zugangsrechte können zwischen Arbeitgeber und Arbeitnehmer vertraglich vereinbart werden.[1805] Der Arbeitgeber oder von ihm beauftragte Personen können sich außerdem vor Einrichtung eines Arbeitsplatzes im häuslichen Umfeld auch die räumliche Situation anschauen und prüfen, inwieweit Datenschutz dort gewährleistet erscheint.[1806] Dennoch ist das Grundrecht des Arbeitnehmers auf Unverletzlichkeit seiner Wohnung nach Artikel 13 GG zu beachten,[1807] da auch ein Arbeitgeber (mittelbar) an die Grundrechte gebunden ist.[1808]

[1804] Vgl. Schlachter in: Noack/Spindler, Unternehmensrecht und Internet, S. 216; Boemke/Ankersen, BB 2000, 1570, 1571.

[1805] Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 9 ff. Vgl. außerdem Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 75.

[1806] Vgl. hierzu auch den Auszug aus einer australischen Telearbeitsvereinbarung in: Basisinformation Telearbeit des Projekts „Online-Forum Telearbeit", S. 39. Die Verpflichtung, Unbefugten den Zugriff auf bestimmte Dokumente zu verwehren, trifft im Übrigen ebenso den Mitarbeiter innerhalb des Unternehmens. Insbesondere in Großraumbüros ist nicht ausgeschlossen, dass Mitarbeiter von Daten Kenntnis nehmen können, die sie gar nichts angehen. Auch hier müssen bestimmte Sicherheitsmaßnahmen getroffen werden, etwa die Verpflichtung, geheime Dokumente stets unter Verschluss zu halten, bestimmte Daten nach der Nutzung sofort zu löschen und nicht zu speichern. Diese Verpflichtung kann auch einem Mitarbeiter im heimischen Bereich auferlegt werden.

[1807] Wedde, Telearbeit, S. 120 ff.; Schlachter in: Noack/Spindler, Unternehmensrecht und Internet, S. 216; die darauf verweist, dass zwar Artikel 13 GG im Arbeitsverhältnis nicht unmittelbar greift, aber über §§ 242, 138 BGB mittelbar zur Anwendung kommen kann. Sofern sich jedoch das Zugangsrecht auf Datenschutzbeauftragte im Sinne von § 38 Abs. 4 BDSG bezieht, dann findet Artikel 13 GG unmittelbar Anwendung, da insofern das Verhältnis zwischen Staat und Bürger berührt wird. Siehe außerdem Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 9 ff.; Basisinformation Telearbeit des Projekts „Online-Forum Telearbeit", S. 57. Vgl. auch Körner, NZA 1999, 1190, 1191 mit dem Hinweis, dass der Grundrechtsschutz nur mittelbar gilt, wenn sich der Arbeitgeber ein Zutrittsrecht vorbehält, da die Wertungen des Grundrechts auch im Rahmen von §§ 242, 138 BGB Anwendung finden.

[1808] Siehe zur mittelbaren Drittwirkung der Grundrechte im Privatrecht Pieroth/Schlink, Grundrechte, Rn. 173 ff. insbesondere Rn. 181; Siehe zur mittelbaren Drittwirkung der Grundrechte im Arbeitsverhältnis Oetker, RdA 2004, 8, 11, Jarass, NJW 1989, 857, 862.

Zwar ist grundsätzlich ein Grundrechtsverzicht zulässig, insbesondere ist zu berücksichtigen, dass es sich bei Artikel 13 GG um ein Grundrecht handelt, welches der persönlichen Entfaltungsfreiheit dient.[1809]
Daher muss von der grundsätzlichen Zulässigkeit eines Verzichts ausgegangen werden, wobei dieser jedoch für den Betroffenen deutlich erkennbar, in voller Kenntnis des Sachverhalts und freiwillig, d.h. nicht unter Druck oder Täuschung, abgegeben werden muss.[1810]
Hierzu wird die Auffassung vertreten, dass dem Arbeitnehmer stets ein Widerrufsrecht bezüglich dieses Grundrechtsverzichts zustehen müsse,[1811] da dieser stets dem Druck unterliegt, sich den Wünschen des Arbeitgebers beugen zu müssen und sich diesen Wünschen nicht entziehen kann.[1812]
Jede Einwilligung ist grundsätzlich frei widerrufbar. Auch wenn das BDSG kein ausdrückliches Widerrufsrecht enthält, ist dies allgemein anerkannt und ergibt sich aus dem allgemeinen Persönlichkeitsrecht desjenigen, der den Widerruf erteilt hat.[1813] In § 4 Abs. 3 TDDSG sowie § 94 TKG ist dieser Grundsatz zudem ausdrücklich geregelt.
Diese Möglichkeit des Widerrufs steht im Besonderen damit im Zusammenhang, dass die Einwilligung auf freiwilliger Basis abgegeben worden sein muss. So steht einer wirksamen Einwilligung der pauschale und zeitlich unbefristete Verzicht der Wahrnehmung der Grundrechte entgegen.[1814] Wichtig ist hierbei die umfassende Information des Betroffenen.[1815] Sofern sich der Einzelne durch umfassende Information über die Tragweite seiner

---

[1809] Vgl. BVerfGE 21, 200, 206 zur Unverzichtbarkeit des Wahlgeheimnisses; BVerfGE 9, 194, 199 zum Rechtsmittelverzicht; BVerGE 65, 1, 41 ff. zur Einwilligung in die Weitergabe persönlicher Daten; OVG Bremen, NJW 1980, 606 ff. zum Fernmeldegeheimnis („Das Grundrecht auf Unverletzbarkeit des Fernmeldegeheimnisses ist nicht unverzichtbar"). Siehe außerdem Pieroth/Schlink, Grundrechte, Rn. 131 ff.; Wesser, NJW 2002, 2138, 2138; Gornig in: v. Mangoldt/Klein/Starck, GG Kommentar, Art. 13 GG Rn. 1.
[1810] Schlachter in: Noack/Spindler, Unternehmensrecht und Internet. S. 216; Pieroth/Schlink, Grundrechte, Rn. 136. Siehe zur Freiwilligkeit einer Einwilligung insbesondere auch Däubler, Internet und Arbeitsrecht, Rn. 332a; Däubler, NZA 2001, 874, 876 sowie die Ausführungen auf S. 363 ff. in dieser Arbeit.
[1811] Vgl. auch Fischer/Schierbaum, CR 1998, 321, 326; Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 10 verweisen darauf, dass auch ein Mitbewohner stets das Recht hat, den Zutritt zu verweigern; LG Düsseldorf, NJW 2003, 1883, 1885; Pieroth/Schlink, Grundrechte, Rn. 139. Siehe zum Widerrufsrecht eines Mitarbeiters im Rahmen von Gesprächsaufzeichnungen Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 299.
[1812] Schlachter in: Noack/Spindler, Unternehmensrecht und Internet. S. 216.
[1813] Vgl. auch Schaar, MMR 2001, 644, 647.
[1814] Wedde, DuD 2004, 169, 172; Dieterich in: Erfurter Kommentar, Einleitung GG Rn. 65. Siehe auch Weichert, NJW 2001, 1463, 1467.
[1815] Wedde, DuD 2004, 169, 172.

Entscheidung im Klaren ist, kommt es im Übrigen nicht mehr auf die „Schwere“ eines Eingriffs an.[1816]

Zwar kann das Widerrufsrecht nicht durch einen Verzicht endgültig ausgeschlossen werden.[1817] Jedoch sind ebenso die Grenzen der Widerrufsmöglichkeit zu beachten. So kann bei Aufrechterhaltung der Rechtsbeziehungen ein Widerruf gemäß den Grundsätzen von Treu und Glauben nur dann erfolgen, sofern die Fortsetzung der Verarbeitung dem Betroffenen objektiv nicht mehr zumutbar ist.[1818]
Insbesondere bei alternierender[1819] Telearbeit ist die Frage zu stellen, aus welchen Gründen sich zukünftig ein Recht des Betroffenen ergeben sollte, von seiner Widerrufsmöglichkeit Gebrauch machen zu dürfen.
Ein Widerruf muss allenfalls dann möglich sein, wenn das Arbeitsverhältnis beendet wird oder sich die Bedingungen bezüglich der Datenverarbeitung, auf deren Grundlage die Einwilligung erfolgte, ändern.[1820] Diesbezüglich wäre denkbar, dass sich die häusliche Situation des Telearbeiters verändern könnte, etwa der Einzug eines neuen Mitbewohners.[1821] Der Entschluss zum Zusammenleben mit anderen hat als Wahrnehmung der durch Artikel 13 GG gewährleisteten Freiheit keinerlei Einfluss auf den Bestand des grundrechtlichen Abwehrrechts.[1822] Ansonsten muss jedoch von einem Ausschluss eines Widerrufsrechts ausgegangen werden, wobei die Angemessenheit der zwischen Arbeitnehmer und Arbeitgeber vereinbarten vertraglichen Regelungen eine zusätzliche Voraussetzung darstellt. Hierzu kann

[1816] LG Düsseldorf, NJW 2003, 1883, 1884; Sprenger/Fischer, NJW 1999, 1830, 1832.
[1817] Schaffland/Wiltfang, BDSG, § 4a BDSG Rn. 27; Bergmann/Möhrle/Herb, Datenschutzrecht, § 4a BDSG Rn. 24.
[1818] Holznagel/Sonntag in: Roßnagel, Handbuch Datenschutzrecht, 4.8 Rn. 66; Simitis in: Simitis, BDSG-Kommentar, § 4a BDSG Rn. 99. Zu beachten ist auch, dass die Widerrufsmöglichkeit für die Zukunft den Nutzer zudem vor überholten Entscheidungen schützen soll (für Teledienste siehe Bizer in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 288); bei der Entscheidung für oder gegen Telearbeit wird der Nutzer jedoch regelmäßig Bedenkzeit haben; Bergmann/Möhrle/Herb, Datenschutzrecht, § 4a BDSG Rn. 24; Schaffland/Wiltfang, BDSG, § 4a BDSG Rn. 26, Siehe auch LG Köln, AfP 1996, 185, 186, welches das Widerrufsrecht immer dann als gegeben ansieht, wenn nach den Umständen des Einzelfalls die Fortwirkung der Einwilligung das Persönlichkeitsrecht des Betroffenen verletzen würde. Siehe zur Wirkung des Widerrufs „für die Zukunft“ OLG Düsseldorf, ZIP 1985, 1318, 1319.
[1819] Siehe zu dem Begriff der alternierenden Telearbeit S. 381.
[1820] Holznagel/Sonntag in: Roßnagel, Handbuch Datenschutzrecht, 4.8 Rn. 66. Siehe in diesem Sinne ebenso Schaffland/Wiltfang, BDSG, § 4a BDSG Rn. 26. LG Köln, AfP 1996, 185, 186.
[1821] Siehe hierzu auch Wesser, NJW 2002, 2138, 2138/2139, wonach Träger dieses Grundrechts jede Person ist, die die Wohnung bewohnt.
[1822] Wesser, NJW 2002, 2138, 2138/2145. Siehe hierzu aber auch Wedde, Telearbeit, S. 125.

etwa gehören, dass sich der Arbeitgeber regelmäßig vorher mit einer angemessenen Frist anmeldet,[1823] es sei denn es würden überwiegende Belange einen sofortigen Besuch rechtfertigen, was jeweils Frage des Einzelfalls ist.[1824]

Insgesamt wirft daher weniger die Frage nach dem Grundrechtsverzicht und dessen Widerrufsmöglichkeiten besondere Probleme auf, sondern inwieweit der Arbeitnehmer freiwillig über das „Ob“ der Telearbeit entscheiden konnte. Die Freiwilligkeit einer Einwilligung kann gegebenenfalls durch Auslegung gemäß §§ 133, 157 BGB ermittelt werden.[1825] Hierbei ist natürlich ebenso die hohe Arbeitslosenzahl zu berücksichtigen, die einen Arbeitnehmer dazu verleiten wird, sich eher mit für ihn unangenehmen Maßnahmen einverstanden zu erklären als generell auf Arbeit zu verzichten. Ist der Bestand des Arbeitsplatzes aber gleichermaßen in den betrieblichen Räumlichkeiten des Arbeitgebers gewährleistet, kann von einem Zwang oder Druck nicht die Rede sein.[1826] Viele Arbeitnehmer entscheiden sich darüber hinaus zu ihrem eigenen Vorteil zur Ausübung von Telearbeit. Denn der Telearbeitsplatz kann in vielen Fällen im Interesse des Arbeitnehmers liegen, beispielsweise der Wunsch nach einem wohnortnahen Arbeitsplatz, flexible Arbeitszeitgestaltung oder die erleichterte Vereinbarkeit von Familie und Beruf.[1827] Diesen Vorteilen der Flexibilität der Arbeitszeit und der Möglichkeit, Beruf und private Interessen besser zu koordinieren, stehen aber die Gefährdung von Verdiensteinbußen und der Verlust sozialer Kontakte gegenüber.[1828]

[1823] Siehe hierzu etwa die Regelung in der Dienstvereinbarung der Hypo-Bank in Basisinformation Telearbeit des Projekts „Online-Forum Telearbeit“, S. 58.

[1824] Basisinformation Telearbeit des Projekts „Online-Forum Telearbeit“ zeigt auf S. 39 ein Beispiel einer Telearbeitsvereinbarung aus Australien (zwischen der Communication Workers´ Union und der Telstra (australische Telekom)), die als Ausnahmefälle für einen Besuch in der Wohnung des Arbeitnehmers einen Tag vor dem vereinbarten Treffen unter anderem Schäden an Arbeitsgeräten oder dringende Sicherheitsbestimmungen nennen, die überprüft werden müssen. Siehe zum Zugangsrecht zur Wohnung auch Gola, NJW 1999, 3753, 3755.

[1825] Wedde, DuD 2004, 169, 172.

[1826] Vgl. zu den Grundsätzen der Telearbeit auch Basisinformation Telearbeit des Projekts „Online-Forum Telearbeit“, S. 48. Außerdem Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 75, der darlegt, dass die Zuweisung eines Telearbeitsplatzes nicht einseitig erfolgen kann, sondern stets die Erforderlichkeit besteht, sich mit dem betroffenen Arbeitnehmer einvernehmlich auf die Einrichtung eines Telearbeitsplatzes zu verständigen.

[1827] Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 1.

[1828] Siehe hierzu Wedde, Telearbeit, S. 11/12, der die Vor-und Nachteile der Telearbeit für die Arbeitnehmer gegenüberstellt.

Auch aus diesem Grund wird im Einzelfall weniger die Angst vor einem Arbeitsplatzverlust im Vordergrund stehen, sondern die Frage, ob die Telearbeitsplätze für den Arbeitgeber in einem solchen Maße vorteilhaft sind, dass er seine Arbeitnehmer zu dieser Arbeitsform in besonderem Maße drängt.[1829] Ist dies nicht feststellbar, so kann ebenso wenig von einer Zwangssituation für den Arbeitnehmer ausgegangen werden. [1830] Anstatt des Einholens einer individuellen Einwilligung der Arbeitnehmer können ebenso Betriebsvereinbarungen getroffen werden oder Regelungen in Tarifverträgen hierzu enthalten sein.[1831] Allerdings muss hierbei stets der Grundsatz des § 75 Abs. 2 BetrVG Berücksichtigung finden.[1832]

Festzustellen ist, dass die Frage der Freiwilligkeit im Einzelfall geprüft werden muss und nicht von vorneherein die Freiwilligkeit der Telearbeit für den betroffenen Arbeitnehmer unterstellt werden kann.[1833] Der Widerruf aus wichtigem Grunde muss außerdem immer zulässig sein.[1834]
Andererseits darf aber nicht vergessen werden, dass der Arbeitgeber nach § 9 BDSG dazu angehalten ist, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen und ein gewisses Datenschutzniveau zu gewährleisten.[1835] Die Betroffenen bzw. die Dritten, deren Daten verarbeitet werden, haben sogar einen Anspruch hierauf.[1836] Daher ist dem Arbeitgeber notwendigerweise daran gelegen, lediglich Mitarbeiter an Telearbeitsplätzen zu beschäftigen, die durch entsprechende Maßnahmen bereit sind, dieses Niveau

[1829] Siehe Wedde, Telearbeit, S. 9/10 zu den zahlreichen Vorteilen für den Arbeitgeber bei der Einführung von Telearbeit.
[1830] Zu berücksichtigen ist aber, dass bei Unwirksamkeit einer erteilten Einwilligung die Interessen des Betroffenen nicht mehr geprüft werden. Die Willenserklärung des Arbeitnehmers ist vielmehr gemäß § 138 BGB nichtig (vgl. Wedde, DuD 2004, 169, 172).
[1831] Siehe Wedde, DuD 2004, 21, 22; Gola, NJW 1996, 3312, 3316, der darauf hinweist, dass die Ausgestaltungen von Telearbeit zum Abschluss erster Tarifverträge und Dienstvereinbarungen geführt haben, die unter anderem dem Umstand Rechnung tragen, dass der häusliche Bereich nunmehr für Betriebsrat und Datenschutzbeauftragten kontrollierbar gemacht werden muss.
[1832] Siehe Wedde, DuD 2004, 169, 174. Vgl hierzu außerdem die Ausführungen auf S. 328/358/364.
[1833] So aber Prinz, NZA 2002, 1268, 1269.
[1834] Gola, NJW 1996, 3312, 3315.
[1835] Siehe auch Wedde, NJW 1999, 527, 534.
[1836] Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 8.

zu unterstützen.[1837] Daran ändert jedoch die Tatsache nichts, dass sich Arbeitnehmer aus freien Stücken zur Telearbeit entscheiden müssen.[1838]

(3) Eingeschränkte Zugriffsrechte

Im Rahmen eines VPN ist von besonderer Bedeutung, ob der Zugriff auf sensible bzw. sensitive Daten zulässig ist.[1839] Die Verarbeitung sensitiver Daten im Wege der Telearbeit wird, wie oben bereits dargestellt, regelmäßig abgelehnt.[1840]
Fraglich ist jedoch, da Telearbeit als Organisationsform auch für so genannte „Guerilla"-Telearbeiter[1841] in Betracht kommt, ob (mobile) Führungskräfte nicht stets ein Interesse daran haben könnten, auf sämtliche personenbezogene Daten uneingeschränkt und von allerorts zugreifen zu können, da sie keinen festen Arbeitsplatz haben.[1842] Daher sollte eine Interessenabwägung zwischen

---

[1837] Diese Maßnahmen müssen ohnehin regelmäßig seitens des Arbeitgebers finanziert werden, so dass der Arbeitnehmer auch keinem finanziellen Druck unterliegt. Vgl. hierzu Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 75 und der Ausführung, dass hierzu neben Kosten für Energie, Abnutzung, Wartung, Reparaturen, Telefon, etc. auch anteilige Mieten gehören. Ebenso Schaub, Arbeitsrechts-Handbuch, § 45 III Rn. 21.
[1838] Ein Widerrufsrecht muss jedoch etwaigen Mitbewohnern zustehen (siehe auch Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 10). Zwar sollte der Arbeitnehmer vor Aufnahme der Telearbeit diesbezüglich eine schriftliche Einwilligungserklärung des/der Mitbewohner(s) dem Arbeitgeber dahingehend vorlegen, dass diese mit einem Zutrittsrecht einverstanden sind und den Arbeitnehmer zur Mitteilung verpflichten, wenn neue Mitbewohner in die Wohnung einziehen. Aber hier ist zu berücksichtigen, dass (anders als im Rahmen der Telearbeit) im Hinblick auf die Mitbewohner zu einem späteren Zeitpunkt nicht ausgeschlossen werden kann, dass sie sich vormals einem faktischen Zwang durch den Arbeitnehmer unterworfen haben, der aber nachträglich wieder rückgängig gemacht werden muss. Hieran ändert auch die räumliche Trennung des betrieblich eingerichteten Arbeitszimmers nicht, da bereits das Betreten des Treppenhauses als Betreten der Privatsphäre und damit unter Artikel 13 GG fallen kann (BVerfGE 96, 245, 246). Der Mitbewohner hätte daher regelmäßig das Recht, insgesamt den Zutritt zu der Wohnung bzw. dem privaten Bereich, zu verweigern, da der Zutritt zu dem betrieblichen Zimmer voraussichtlich durch andere private Räumlichkeiten führen wird.
[1839] Siehe zum Begriff der sensiblen Daten S. 403.
[1840] Siehe Gola/Schomerus, BDSG, § 9 BDSG Rn. 17, die auf den 15. Tätigkeitsbericht des Landesdatenschutzbeauftragten Bremen, S. 129 verweisen. Dort wird ein grundsätzliches Verbot der Verarbeitung von sensiblen Daten auf tragbaren PC´s bzw. Laptops ausgesprochen. Auch Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 11 lehnen die Verarbeitung von Sozial-, Personal-, Steuer- und Gesundheitsdaten im Rahmen der Telearbeit als ungeeignet ab.
[1841] Siehe zu diesem Begriff Fn. 1628.
[1842] Der Trend der Unternehmen zur Mobilität kann zwar selbstverständlich keine Rechtfertigung für eine solche „globale" Datenverarbeitung sein. Zumindest kann aber in diesem Zusammenhang die Frage aufgeworfen werden, inwieweit gegebenenfalls eine Güterabwägung zwischen dringenden Interessen des Unternehmens an wirtschaftlicher Entfaltungsfreiheit nach Artikel 2 Abs. 1 GG (gegebenenfalls in Verbindung mit Artikel 19 Abs. 3 GG) und den Grundrechten aus Artikel 12 GG des Mitarbeiters an freier Berufsausübung einerseits sowie das Recht des Dritten an informationeller Selbstbestimmung andererseits stattfinden müsste.

dem Recht des Unternehmers auf wirtschaftliche Betätigungsfreiheit[1843] und dem Recht des Dritten auf informationelle Selbstbestimmung stattfinden. Die Verarbeitung sensibler Daten sollte dementsprechend im Rahmen von Telearbeit grundsätzlich nicht von vorneherein verneint werden.[1844] Bei Telearbeit geht es daher nicht nur um die Sicherung der Grundrechte des Arbeitnehmers und die des Arbeitgebers, da dessen Tätigkeit als Unternehmer wesentlicher Bestandteil seines Persönlichkeitsrechts ist,[1845] sondern auch und insbesondere um die Interessen des Dritten bzw. des Betroffenen, dessen Daten verarbeitet werden.

Zu beachten ist hierbei stets, dass die Interessen des Betroffenen am Ausschluss der Verarbeitung aufgrund der Vorgaben in § 4 BDSG im Zweifelsfall höherrangig zu bewerten sind.[1846] Dementsprechend wäre unter Berücksichtigung der „berechtigten Interessen“ sowie des gegebenenfalls bestehenden „überwiegenden Interesses“ des Betroffenen, zu prüfen, ob tatsächlich im Einzelfall ein Zugriff erfolgen „muss“.[1847] Bei der Beurteilung dieser Notwendigkeit ist ebenfalls den besonderen Umstände der betrieblichen Gestaltung im Einzelfall Rechnung zu tragen. So kann der Unternehmer nicht unter allen Umständen gezwungen sein, die Verarbeitung von sensitiven Daten auf einen einzigen Standort zu begrenzen. Dies gilt gerade hinsichtlich der oben angesprochenen Form der „Guerilla-Tätigkeit“. Um die Interessen der Betroffenen zu wahren, kommt allerdings eine solche Verarbeitung nur ausnahmsweise und gegebenenfalls zeitlich begrenzt in Betracht. Insbesondere

[1843] Als einschlägige Grundrechte der unternehmerischen Betätigungsfreiheit kommen im Übrigen Art. 2 Abs. 1 GG, Art. 12 GG sowie Art. 14 GG in Betracht (vgl. hierzu Dieterich in: Erfurter Kommentar, Art. 14 GG Rn. 9; Wieland in Dreier, GG-Kommentar, Art. 14 GG Rn. 184; Degenhart, JuS 1990, 161, 169). In der Literatur wird ein umfassender Schutzbereich der „Wirtschaftsfreiheit“, der gleichermaßen den Schutzbereich von Art. 2, 12 und 14 GG erfasst, abgelehnt (Dieterich in: Erfurter Kommentar, Art. 14 GG Rn. 9; Wieland in: Dreier, GG-Kommentar, Art. 14 GG Rn. 184). Das Bundesverfassungsgericht hat die unternehmerische Betätigungsfreiheit in seinen Entscheidungen überwiegend dem Schutzbereich des Art. 2 Abs. 1 GG zugeordnet (siehe zur wirtschaftlichen Betätigungsfreiheit die Entscheidungen BVerfGE 91, 207, 221 und BVerfGE 98, 218, 259 einerseits sowie zur unternehmerischen Handlungsfreiheit die Entscheidungen BVerfGE 50, 290, 366 und BVerfGE 65, 196, 210 andererseits), teilweise auch dem Schutz der Berufsfreiheit gemäß Art. 12 Abs. 1 GG unterstellt (vgl. BVerfGE 81, 242, 254/255 zur Vertragsfreiheit; siehe zur Vertragsfreiheit als Teil der wirtschaftlichen Betätigungsfreiheit BVerfGE 97, 267, 303).

[1844] Zur Zulässigkeit der Verarbeitung sensibler Daten siehe Zilkens/Wehrhahn, RDV 1999, 60, 63.

[1845] Vgl. Raffler/Hellich, NZA 1997, 862, 862.

[1846] Siehe auch Hoeren in: Roßnagel, Handbuch Datenschutzrecht, 4.6 Rn. 33.

[1847] Dies gilt insbesondere, da „die berechtigten Interessen“ Anknüpfungspunkt für eine nur im Ausnahmefall zulässige Datenverarbeitung sind (vgl. Scholz in: Roßnagel, Handbuch Datenschutzrecht, 9.2 Rn. 91).

sind hier besonders hohe Anforderungen an die technischen und organisatorischen Maßnahmen zu stellen,[1848] wobei besonders strenge Maßstäbe im Hinblick darauf anzulegen sind, auf welche Personengruppen bzw. Mitarbeiter und zu welchen Zwecken der Zugriff zu begrenzen ist.
In diesem Zusammenhang ist die Frage zu stellen, ob einem Mitarbeiter bzw. Führungsperson auf sämtliche (sensiblen) personenbezogenen Daten Zugriffsrechte eingeräumt werden „müssen“. So kommen auch eingeschränkte Zugriffsrechte, beschränkt auf gewisse Dateien oder Daten in Betracht.
Es muss einerseits sichergestellt sein, dass lediglich Mitarbeiter, die regelmäßig aufgrund ihrer besonderen Führungsrolle nicht mehr zwangsläufig tagtäglich in dem Unternehmen an einem festen Platz arbeiten, dennoch ihren Aufgaben nachkommen können.[1849] Andererseits sind die Interessen des Betroffenen ausreichend zu wahren.
Diesbezüglich könnte als (eine) organisatorische Maßnahme eine Vereinbarung dahingehend getroffen werden, dass sensible Daten nur solange auf dem mobilen Rechner gespeichert werden, wie sie zur Erfüllung der Aufgabe erforderlich sind.[1850] Die Freigabe auf gewisse Dateien könnte hier auch zeitweise erfolgen, ohne einen generellen Zugriff zu erlauben. Darüber hinaus kommt ebenfalls die Möglichkeit des Application Service Providing in Betracht.[1851] Wichtig ist, dass im Hinblick die Datenverarbeitung auf dem jeweiligen Rechner ein Maximum an Schutzmaßnahmen getroffen wird. Hier könnte seitens des VPN-Auftraggebers bzw. Arbeitgebers für die Arbeitnehmer entsprechende Schulungen durchgeführt, etwa im Hinblick auf die sinnvolle Passwortvergabe am Arbeitsplatz. Auch müsste der Arbeitnehmer darauf sensibilisiert werden, den Rechner nicht Familienangehörigen zu überlassen.

[1848] Siehe oben S. 407 ff., wobei hier vor allem besonderes Augenmerk auf die Löschungspflichten, den unbeobachteten Zugriff sowie die ausreichende Datenverschlüsselung bei der Übermittlung gelegt werden muss. Im Übrigen kommt § 38 Abs. 4 BDSG bei mobilen Geräten von vorneherein nicht in Betracht, wobei aber der Arbeitnehmer dazu verpflichtet werden könnte, auf Verlangen der zuständigen Behörde sein Laptop zur Verfügung zu stellen.
[1849] Vgl. auch Dammann in: Simitis, BDSG-Kommentar, § 28 BDSG Rn. 106/115 zu den Verarbeitungsschranken und dem Hinweis (Rn. 115), dass Daten innerhalb der verantwortlichen Stelle nicht frei zirkulieren dürfen.
[1850] Ein Geschäftsführer, der sich oft auf Dienstreisen befindet, kann beispielsweise ein Interesse daran haben, persönliche Daten von Bewerbern zu prüfen (u.U. auch Schwerbehinderteneigenschaft).
[1851] Siehe zu Application Service Providing S. 74/81.

Außerdem sollte der Zugriff stets nur seitens des Clients auf ein mittels Gateway gesicherten Unternehmensnetz erfolgen, bei welchem sichergestellt ist, dass personenbezogene Daten nicht auf dem selben Rechner verarbeitet werden, auf welchem ebenso die Nutzerverwaltung stattfindet, da dies einen zusätzlichen Angriffspunkt auf das Unternehmensnetz und damit auf die dort gespeicherten personenbezogenen Daten bietet.[1852]

Zu berücksichtigen ist hierbei außerdem, dass sich ein Zugriffsrecht auf sensitive Daten für bestimmte Mitarbeiter von vorneherein verneinen lässt. Beispielsweise haben Vertriebsmitarbeiter regelmäßig lediglich ein Interesse daran, auf Kundennamen, Kundenanschriften, etc. auch von unterwegs zugreifen zu können.[1853] Der Zugriff auf sensible Daten wird hingegen nicht erforderlich sein.

Ebenso wenig kommt selbstverständlich aus Gründen der Bequemlichkeit die zulässige Verarbeitung sensibler Daten auf heimischen Rechnern oder Laptops in Betracht. Ein Mitarbeiter aus der Personalabteilung, der seinen festen Arbeitsplatz im Büro hat, muss nicht notwendigerweise am Sonntag von zu Hause aus, seine Arbeit erledigen, sondern könnte entsprechende Überstunden im Büro machen.

Es ist also stets besonderes Augenmerk darauf zu legen, ob im Sinne von § 28 Abs. 1 Nr. 2 BDSG nicht das Interesse des Betroffenen an dem Ausschluss der Verarbeitung sensitiver Daten überwiegt,[1854] wobei dieses Interesse nicht per se überwiegt, sondern nur dann wenn die Auswahl der zugriffsberechtigten Personen sowie die technischen und organisatorischen Maßnahmen im Einzelfall nicht an strenge und enge Voraussetzungen gebunden sind.

[1852] Vgl. auch die Ausführungen in Fn. 227/228.

[1853] Die Ausführungen von Ruppmann, Der konzerninterne Austausch personenbezogener Daten, S. 39 enthalten den Hinweis, dass Daten von Kunden oder Lieferanten zu den so genannten gemischten Daten zählen. Dies bedeutet, dass hier sowohl unternehmens- als auch personenbezogene Daten anfallen, wobei aber letztendlich die sachbezogenen Daten der Vertragserfüllung dienten. Zu diesen Ausführungen von Ruppmann muss weiterhin ergänzend darauf hingewiesen werden, dass ebenso bei einer juristischen Person nicht nur sachbezogene Daten anfallen, sondern vielfach personenbezogene Daten der einzelnen Mitarbeiter dieses Unternehmens. Hier kann etwa das Beispiel angeführt werden, dass ein Vertriebsmitarbeiter gegebenenfalls auf Namen, E-Mail-Adresse, Handynummer, etc. eines Ansprechpartners bei dem jeweiligen Unternehmen (welches Vertragspartner ist) zugreifen muss. Dann würde es sich sowohl um sachbezogene Angaben des Unternehmens als auch um personenbezogene Daten des Mitarbeiters handeln.

[1854] Da der Betroffene bei sensiblen Daten (§ 3 Abs. 9 BDSG) nach § 4a Abs. 3 BDSG ohnehin in die Speicherung einwilligen muss (unter der Ausnahme des § 28 Abs. 7 BDSG), könnte in diesem Rahmen ebenfalls daran gedacht werden, den Betroffenen über die Verwendung seiner Daten umfassend aufzuklären und ihm entweder ein Widerspruchsrecht zuzubilligen oder aber sein Einverständnis zu der Telearbeit explizit einzuholen.

Diese Überlegungen zu den sensiblen Daten gelten im Übrigen für jede Art von personenbezogenen Daten.
Es muss stets im Einzelfall geprüft werden, ob der jeweilige Mitarbeiter bzw. Telearbeiter ein berechtigtes Interesse hat, auf die jeweiligen Daten zuzugreifen oder ob nicht schutzwürdige Interessen des Betroffenen überwiegen. Der Ausschluss eines Zugriffsrecht kann hier sowohl mangels ausreichender technischer oder organisatorischer Maßnahmen in Betracht kommen, als auch dadurch, dass der einzelne Mitarbeiter die jeweiligen personenbezogenen Daten für die Ausführung seiner Arbeit nicht benötigt bzw. aufgrund seines „festen" Arbeitsplatzes im Unternehmen nicht notwendigerweise im heimischen Bereich benötigt.

bb. Auftragsdatenverarbeitung

Auftragsdatenverarbeitung unterfällt neben der Funktionsübertragung dem Begriff des Outsourcing,[1855] wobei die Zulässigkeit der Datenweitergabe an den Auftragnehmer an den Zulässigkeitsvoraussetzungen des § 28 Abs. 1 Nr. 2 BDSG zu messen ist.[1856]
In diesem Zusammenhang ist festgestellt worden, dass die Voraussetzungen des § 11 BDSG innerhalb der Interessenabwägung des § 28 Abs. 1 Nr. 2 BDSG zu prüfen sind.
Für den speziellen Bereich der „Datenweitergabe" über das Internet muss weiterhin entsprechend der obigen Überlegungen zur Telearbeit im häuslichen Bereich zusätzlich zu der in § 11 BDSG bereits geregelten sorgfältigen Auswahl des Auftragnehmers ebenso die besondere Unsicherheit des Internet innerhalb der Interessenabwägung gemäß § 28 Abs. 1 Nr. 2 BDSG berücksichtigt werden.
Der VPN-Auftraggeber muss nicht nur darauf achten, dass bei seinem Auftragnehmer die Datensicherheit gewährleistet ist. Er muss wegen der unsicheren Struktur des Internet darüber hinaus die unterschiedlichen

[1855] Siehe hierzu S. 382.
[1856] Vgl. auch Evertz in: Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck, Cyberlaw, S. 77, der für Arbeitnehmer darauf hinweist, dass deren Erfassung und Verarbeitung für eigene Zwecke im Rahmen eines Personalinformationssystems (Personal- und Lohnbüro) unter den Voraussetzungen des § 28 Abs. 1 Nr. 1 und Nr. 2 BDSG dann zulässig ist und keine internetspezifischen Probleme erzeugt, solange sichergestellt ist, dass auf diese Daten von außen nicht zugegriffen werden kann.

Verschlüsselungstechniken als technische Maßnahmen in seine Überlegung mit einbeziehen, sowie die Frage, ob der Zugriff auf sensible Daten erforderlich ist. Der VPN-Auftraggeber, der gemäß § 11 BDSG für den Datenschutz verantwortlich ist, muss für die notwendigen Verschlüsselungsmaßnahmen Sorge tragen und Tochterunternehmen, Zweigstellen oder Externe wie Lieferanten[1857] auf diese Verschlüsselung nicht nur hinweisen, sondern ihnen entsprechende Techniken zur Verfügung stellen.

Unerheblich ist in diesem Zusammenhang, ob Externe, Tochterunternehmen oder Zweigstellen rechtlich selbständig sind.[1858] Denn es kommt allein auf die konkrete und inhaltliche Ausgestaltung der Datenverarbeitung an. Ist dieser zu entnehmen, dass es sich um eine Auftragsdatenverarbeitung handelt, wird insbesondere das Eigeninteresse des VPN-Auftraggebers an den Daten nicht aufgegeben.[1859]

Entsprechend der Telearbeit im häuslichen Bereich ist gleichermaßen bei der Auftragsdatenverarbeitung im Rahmen eines VPN eine Pflicht zur Verschlüsselung von personenbezogenen Daten eines VPN im Rahmen eindeutig zu normieren.[1860] Aufgrund der technischen Möglichkeiten und Standards stellen Verschlüsselungsmaßnahmen heutzutage kein Problem dar.[1861] Insbesondere wird die Bedienung von Kryptographieprogrammen einfacher und der Stand der Technik entwickelt sich fort,[1862] womit die Anforderungen an die Zulässigkeit von Telearbeit wachsen.

[1857] Schlachter in: Noack/Spindler, Unternehmensrecht und Internet, S. 215; Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 6.

[1858] Insoweit missverständlich Niedermeier/Schröcker, RDV 2001, 90, 92, wobei sich aber im Verlaufe ihrer Ausführungen ergibt, dass auch eine Tochtergesellschaft sowohl Auftragsdatenverarbeitung als auch Funktionsübertragung wahrnehmen kann, und zwar unabhängig von der Rechtsform bzw. rechtlichen Selbständigkeit. Ebenso vage Schaffland/Wiltfang, BDSG, § 10 BDSG Rn. 1a, die erläutern, dass das BDSG generell auf die juristische (und nicht wirtschaftliche) Einheit als speichernde Stelle abstellt, was bedeute, dass Dritter jede Stelle oder Person außerhalb der juristischen Einheit (also z.B. Konzern-Mutter-AG oder Tochter-GmbH) sei. Unter der Kommentierung des § 3 BDSG Rn. 54 wird von den Verfassern aber nochmals klar gestellt, dass keine Datenübermittlung an Dritte vorliegt, sofern die Datenweitergabe an das Konzernunternehmen ausschließlich wegen der Datenverarbeitung im Auftrag erfolgt.

[1859] Gola/Schomerus, BDSG, § 28 BDSG Rn. 4; vgl. ebenso Gola/Wronka, RDV 1994, 157, 164, die eine Abgrenzung zwischen Auftragsdatenverarbeitung und eigener Datenherrschaft anhand von Direktmarketingmaßnahmen und der Weitergabe von Kundenadressen vornehmen.

[1860] Siehe zur Telearbeit im häuslichen Bereich die Ausführungen auf S. 412 ff.

[1861] Vgl. auch Fn. 1784.

[1862] Backu, ITRB 2003, 251, 253.

Daher muss auch bei der Auftragsdatenverarbeitung der Einsatz von Verschlüsselungen gefordert werden, wobei wiederum die Frage zu stellen ist, inwieweit neben der Datenverschlüsselung zusätzliche Schutzmaßnahmen, wie sie IPSec bietet, verwendet werden müssen.[1863]

Im Unterschied zur Telearbeit im häuslichen Bereich kann allerdings bei Standortvernetzung (wenn die weiteren Datenverarbeitungen in den Räumlichkeiten des VPN-Auftraggebers stattfinden) oder bei Zugriffen durch andere Unternehmen innerhalb ihrer Betriebsstätten, die Verarbeitung sensibler Daten unter erleichterten Voraussetzungen in Betracht kommen. Denn Telearbeit wird für die Verarbeitung sensibler Daten regelmäßig nur dann strikt abgelehnt, sofern es sich um die Datenverarbeitung im häuslichen Bereich handelt.[1864] Findet der Abruf jedoch in einem Betrieb bzw. Unternehmen statt, so bedeutet dies, dass die Unsicherheit des heimischen Bereichs nicht gegeben ist.[1865]

Zwar bleibt die Unsicherheit der Datenübertragung über das Internet bestehen und es wird absoluten Schutz hinsichtlich einer Verschlüsselungstechnik nie geben.[1866] Jedoch wird es diesen Schutz ebenso wenig geben, sofern die Datenverarbeitung im Betrieb selbst stattfindet.

So wie Datenschlüssel grundsätzlich zu dechiffrieren sind, können auch die Sicherheitsvorrichtungen eines Betriebs umgangen werden, und ist das Schloss jedes Serverraums grundsätzlich der Möglichkeit ausgesetzt, aufgebrochen zu werden. Insbesondere aufgrund der Möglichkeiten der heutigen Verschlüsselungstechniken und deren stetiger Fortentwicklung (beispielsweise Daten verschlüsselt in ein anderes Datenpaket mit neuem IP-Header

---

[1863] Siehe hierzu die Ausführungen auf S. 409 ff.

[1864] Hierbei ist aber zu beachten, dass es gesetzliche Beschränkungen für die Verarbeitung sensitiver Daten gibt. So verbietet Artikel 26 Abs. 4 S. 5 Bayerisches Krankenhausgesetz die externe Verarbeitung medizinischer Patientendaten, wobei die Verfassungsmäßigkeit einer solchen Regelung seitens des Bundesverfassungsgerichts als verfassungsgemäß bestätigt wurde (BVerfG, NJW 1991, 2952, 2953). Das Bayerische Verfassungsgericht vertritt hier die Ansicht, dass der Gesetzgeber den Schutz der Patienten vor Weitergabe ihrer medizinischen Daten an Stellen außerhalb des Krankenhauses höher gewichten darf als das Interesse privater Dritter, diese Daten in ihrem Unternehmen bearbeiten bzw. hieran die Mikroverfilmung vornehmen zu dürfen (BayVerfG, NJW 1989, 2939, 2940).

[1865] Siehe hierzu Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 8, insbesondere Fn. 14.

[1866] Vgl. oben S. 39 sowie S. 414, wo in Fn. 1794 ebenfalls auf die organisatorischen Sicherheitsanforderungen innerhalb eines Krankenhauses verwiesen worden ist.

einzupacken)[1867] muss die Übertragung sensibler Daten über das Internet grundsätzlich zulässig sein, da die Netzunsicherheit damit überbrückt werden kann.[1868]
Dabei ist der VPN-Auftraggeber auch nicht von der Prüfungspflicht befreit, welche Schutzmaßnahmen organisatorischer Art im Einzelfall darüber hinaus zu beachten sind. So muss etwa gemäß § 11 BDSG beim Auftragnehmer bei der „weiteren“ Datenverarbeitung für entsprechende Datensicherungsmaßnahmen- und systeme gesorgt sein. Diese Maßnahmen hat er konkret und schriftlich auszugestalten.[1869]
Insbesondere ist hier ebenso der Grundsatz der Datenvermeidung gemäß § 3a BDSG zu berücksichtigen, so dass zu prüfen ist, inwieweit es im Einzelfall dem VPN-Auftraggeber zumutbar ist, Application Service Providing anzubieten.[1870] Denn durch das Arbeiten auf den Systemen des VPN-Auftraggebers wird verhindert, dass personenbezogene Daten auf mehreren technischen Systemen entstehen, was ebenso zur Datenvermeidung beiträgt.

cc. Funktionsübertragung

Im Rahmen der Funktionsübertragung ist zu beachten, dass bei der Interessenabwägung des § 28 Abs. 1 Nr. 2 BDSG ebenfalls eine sorgfältige Auswahl des Auftragnehmers seitens des VPN-Auftraggebers erforderlich ist. Die Funktionsübertragung stellt ein „Mehr“ zur Auftragsdatenverarbeitung da. Bei einer Funktionsübertragung müssen die Nutzer des VPN (Externe, Zweigstellen oder Tochterunternehmen) eigenständig für die Einhaltung des Datenschutzes Sorge tragen, etwa die Maßnahmen nach § 9 BDSG sicherstellen, gegebenenfalls einen Datenschutzbeauftragten[1871] gemäß § 4 f BDSG bestellen und bei der Datenverarbeitung für eigene Zwecke ebenso die Voraussetzungen des § 28 BDSG beachten.[1872] Hier geben sich insoweit keine Unterschiede zu den datenschutzrechtlichen Pflichten des VPN-

[1867] Siehe oben S. 39 ff.
[1868] Vgl. S. 236, insbesondere 1014 und die Hinweise von Schneider, MMR 1999, 571, 575.
[1869] Vgl. hierzu auch die folgenden Ausführungen auf S. 436 ff.
[1870] Siehe zu Application Service Providing S. 74/81.
[1871] Siehe zum betrieblichen Datenschutzbeauftragten Wedde, Telearbeit, S. 130.
[1872] Zum Aufgabenspektrum des betrieblichen Datenschutzbeauftragten siehe auch Breinlinger, RDV 1995, 7 ff., die auf S. 9 darauf verweist, dass sich das Bild der internen Kontrolle im Unternehmen nicht besonders positiv darstellt, insbesondere wenn als Maßstab die hohen Anforderungen des Bundesdatenschutzgesetzes ernst genommen werden.

Auftraggebers, da beide eigenständig für die Einhaltung des Datenschutzes gegenüber dem Betroffenen bzw. Dritten verantwortlich sind. Daher sind Externe, die Zweigstelle oder das Tochterunternehmen aufgrund der mit einer Funktionsübertragung verbundenen eigenständigen datenschutzrechtlichen Pflichten für das ausreichende Datenschutzniveau und die Verwendung der notwendigen Verschlüsselungssysteme verantwortlich.[1873] Letzteres muss natürlich in Absprache mit dem VPN-Auftraggeber geschehen, da die technischen Systeme bei einem VPN notwendigerweise aufeinander abgestimmt werden müssen.

Von diesem (weiteren) Verlauf der Datenverarbeitung ist aber die Zulässigkeit der Datenweitergabe an sich zu unterscheiden, die an den Voraussetzungen des § 28 Abs. 1 Nr. 2 BDSG zu messen ist. Ist bereits absehbar, dass der Auftragnehmer organisatorische und technische Maßnahmen nach § 9 BDSG nicht ausreichend erfüllen kann, sprechen die schutzwürdigen Interessen des Betroffenen bereits im Vorfeld gegen eine Weitergabe der Daten an den Dritten gemäß § 28 Abs. 1 Nr. 2 BDSG. In diesem Falle kann somit eine Übermittlung der Daten nur mit Einwilligung des Betroffenen gemäß § 4a BDSG stattfinden. Entsprechendes gilt, wenn die Datenübermittlung für eigene Zwecke des Nutzer erfolgt.[1874] Dies bedeutet daher insgesamt, dass eine Funktionsübertragung gemäß § 28 Abs. 1 Nr. 2 BDSG (d.h. ohne Einwilligung des Betroffenen!) lediglich in Betracht kommen kann, wenn die Datenverarbeitung beim Nutzer ausschließlich für eigene Zwecke des VPN-Auftraggebers erfolgt und der Nutzer darüber hinaus ausreichende technische und organisatorische Schutzmaßnahmen gemäß § 9 BDSG trifft.

In rechtspolitischer Hinsicht ist aber anzumerken, dass die gesetzliche Regelung sehr weitgehend ist. § 28 Abs. 1 Nr. 2 BDSG lässt zwar die Übermittlung für eigene Zwecke zu, sofern die schutzwürdigen Interessen des Betroffenen nicht dagegen sprechen. Diesbezüglich ist jedoch anzumerken, dass das Gesetz die Auftragsdatenverarbeitung gemäß § 11 BDSG bereithält. Gemäß § 11 BDSG muss der Auftraggeber Kontroll- und Weisungsbefugnisse gegenüber dem Auftragnehmer ausüben und die Einhaltung des Datenschutzes beim Verarbeiter überwachen. Wird nun durch § 28 Abs. 1 Nr. 2 BDSG ebenso

[1873] Vgl. hierzu auch Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 7.
[1874] Es gibt bei der Datenverarbeitung kein Konzernprivileg. Siehe hierzu Däubler, Gläserne Belegschaften?, Rn. 450 ff.; Simitis in: Simitis, BDSG-Kommentar, § 2 BDSG Rn. 150 ff.

die Übermittlung von Daten zugelassen, so würde in letzter Konsequenz § 11 BDSG und insbesondere dessen Schriftformerfordernis ausgehebelt werden.[1875] In diesem Sinne ist daher in rechtspolitischer Hinsicht die Streichung des Übermittlungstatbestand gemäß § 28 BDSG zu fordern, so dass der Auftraggeber verpflichtet ist, die strengen Regelungen des § 11 BDSG zu befolgen oder aber bei der Datenübermittlung die ausdrückliche Einwilligung des Betroffenen gemäß § 4a BDSG einzuholen.

dd. Besondere Ausführungen zur zweckgebundenen Verwendung

Im Personenverhältnis zwischen VPN-Auftraggeber und Nutzer wurde dargestellt, dass in Abhängigkeit von der Verwendungsabsicht des Nutzers des VPN die rechtliche Einordnung der VPN-Kommunikation sowohl als Teledienst[1876] gemäß § 2 Abs. 1 TDG als auch als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG in Betracht kommen kann.[1877] Im Anschluss an diese Einordnung wurde geprüft, welche Auswirkung dies auf den datenschutzrechtliche Umgang mit den personenbezogenen Daten des Nutzers hat.[1878] Im Folgenden wird nun dargestellt, inwieweit die im Personenverhältnis „VPN-Auftraggeber/Nutzer“ getroffenen Feststellungen ebenso in diesem Personenverhältnis (VPN-Auftraggeber/Betroffener) relevant sind.

aaa. Teledienst

Sofern der VPN-Auftraggeber Informationen bzw. Inhalte zum Abruf bereitstellt, ist oben festgestellt worden, dass es sich um einen inhaltsbezogenen Dienst bzw. um einen Teledienst handelt.[1879]
Für Teledienste enthält § 10 BDSG eine Sonderregelung über die Zulässigkeit eines solchen Abrufverfahrens. Die Anwendbarkeit von § 28 Abs. 1 Nr. 2 BDSG steht hierzu nicht im Widerspruch, da die Zulässigkeit der Übermittlung von Daten in § 10 BDSG vorausgesetzt wird und ausschließlich festlegt, unter

[1875] Siehe zum Schriftformerfordernis Gola/Schomerus, BDSG; § 11 BDSG Rn. 17; Schaffland/Wiltfang, BDSG, § 11 BDSG Rn. 9a.
[1876] Siehe S. 310 ff.
[1877] Siehe S. 312 ff.
[1878] Siehe S. 335 ff.
[1879] Siehe S. 310 ff., wobei in seltenen Fällen auch ein Mediendienst gemäß § 2 Abs. 1 MDStV in Betracht kommen kann.

welchen Voraussetzungen die Datenverarbeitung im automatisierten Abrufverfahren zulässig ist und nicht die Zulässigkeit der Übermittlung als solche regelt.[1880]

§ 10 BDSG bestimmt die Voraussetzungen für die Zulässigkeit der Einrichtung eines automatisierten[1881] (Online)-Abrufverfahrens[1882] für den öffentlichen[1883] und nicht öffentlichen Bereich.[1884] Die Zulässigkeit aller (künftig) im Rahmen dieses Verfahrens getätigten Abrufe bedarf aber gemäß § 10 Abs. 1 S. 2 BDSG weiterhin der Zulässigkeitsregelungen des BDSG, wie etwa § 28 BDSG für den nicht-öffentlichen Bereich,[1885] oder der Landesdatenschutzgesetze.[1886]

[1880] Schaffland/Wiltfang, BDSG, § 10 BDSG Rn. 4. Lediglich das Bereithalten der Daten wird durch § 10 BDSG geschützt und nicht mehr durch §§ 15-17, 28, 29 BDSG (vgl. Auernhammer, BDSG, § 3 BDSG Rn. 38). Siehe außerdem Gola/Schomerus, BDSG, § 10 BDSG Rn. 7, die darauf verweisen, dass sich § 10 BDSG auf den vom TDDSG nicht geregelten Inhalt der Informationen bezieht und die Daten Dritter und nicht die Daten der Nutzer des Teledienstes schützen möchte.

[1881] § 10 BDSG gilt ausdrücklich nur für automatisierte Abrufverfahren, wobei im Übrigen nicht automatisierte Abrufverfahren in der heutigen Praxis sehr selten sind (siehe hierzu Ehmann in: Simitis, BDSG-Kommentar, § 10 BDSG Rn. 31).

[1882] Auerhammer, BDSG, § 10 BDSG Rn. 2 verweist darauf, dass § 10 BDSG nur für Online-Verfahren der speichernden Stelle mit Dritten gilt.

[1883] Im Hinblick auf den öffentlichen Bereich müssen VPN-Betreiber die vorrangigen landesdatenschutzrechtlichen Regelungen (zum Vorrang der landesgesetzlichen Regelungen gegenüber dem BDSG siehe Schaffland/Wiltfang, BDSG, § 1 BDSG Rn. 38) beachten, die allesamt für die Verarbeitung personenbezogener Daten durch öffentliche Stelle eigene Regelungen vorsehen. So regeln einzelne Landesdatenschutzgesetze, dass ein automatisiertes Abrufverfahren nur eingerichtet werden darf, wenn eine Rechtsvorschrift dies ausdrücklich zulässt.

[1884] Auernhammer, BDSG, § 10 BDSG Rn. 2.

[1885] Vgl. Auernhammer, BDSG, § 10 BDSG Rn. 7, der unter Rn. 13 und Rn. 14 außerdem darauf hinweist, dass die abrufende Stelle darauf achten muss, dass der Abruf jeweils durch eine Zulässigkeitsvorschrift gedeckt ist, und die speichernde Stelle sich grundsätzlich darauf verlassen können soll, dass sich die Datenempfänger an die getroffenen Vereinbarungen (§ 28 Abs. 2 S. 2 BDSG) und die Zulässigkeitsnormen (§ 28 Abs. 1 S. 2 BDSG) halten werden.

[1886] Siehe etwa § 15 Berliner Datenschutzgesetz, welches in Abs. 1 regelt, dass ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Behörden oder sonstige öffentliche Stellen nur eingerichtet werden darf, wenn ein Gesetz dies ausdrücklich zulässt. In § 15 Abs. 3 Berliner Datenschutzgesetz ist zudem normiert, dass personenbezogene Daten für Stellen außerhalb des öffentlichen Bereichs zum automatisierten Abruf nicht bereitgehalten werden dürfen. Entsprechendes regeln § 11 Abs. 1 und Abs. 4 Hamburgisches Datenschutzgesetz sowie § 9 Abs. 1 und Abs. 5 Datenschutzgesetz Nordrhein-Westfalen. § 15 Abs. 1 Hessisches Datenschutzgesetz regelt, dass vor der Einrichtung eines automatisierten Verfahrens, welches mehreren datenverarbeitenden Stellen zur Verfügung steht, der Hessische Datenschutzbeauftragte zu hören ist. Siehe hierzu auch Gola/Schomerus, BDSG, § 10 BDSG Rn. 19; Schaffland/Wiltfang, BDSG, § 10 BDSG Rn. 1. Es kann sich hier insbesondere auch die Frage stellen, inwieweit es eine Umgehung des jeweiligen Landesrechts darstellt, wenn beispielsweise eine öffentliche Stelle des Landes Berlin, die Daten an einen Server in Bayern übermittelt, um von dort letztendlich den Datenabruf zu ermöglichen (in der nachfolgenden Fußnote wird auf die Regelungen des Bayerischen Datenschutzgesetzes verwiesen, die keine Zulässigkeit durch separate eine separate Rechtsvorschrift für das automatisierte Abrufverfahren verlangen, so dass insoweit mildere Zulässigkeitsvoraussetzungen Anwendung finden). Richtigerweise sollte jedoch nicht auf den Server-Standort abgestellt werden, sondern auf den Sitz der Stelle, die das automatisierte Verfahren einrichtet, da die Stelle, welche die Datenverarbeitung betreibt, Behörde, etc. des jeweiligen Landes ist (und bleibt) und sämtliche

In diesem Zusammenhang sind insbesondere § 10 Abs. 2 BDSG und § 10 Abs. 4 BDSG von Bedeutung, in denen nochmals gesonderte Kontrollverfahren und die Verantwortung für die Zulässigkeit des einzelnen Abrufs festgelegt werden. Dies bedeutet, dass bei einer Funktionsübertragung zusätzlich im Rahmen eines VPN und der damit verbundenen Datenübermittlung (an Dritte), also einer Datenweitergabe an (natürliche oder juristische) Personen, die keine Datenverarbeitung im Auftrag gemäß § 11 BDSG erledigen,[1887] eine zweistufige Zulässigkeitsprüfung vorgesehen ist, wobei in einem ersten Schritt zu entscheiden ist, ob die Einrichtung des Abrufverfahrens als solches, etwa durch ausreichende technische und organisatorische Maßnahmen nach § 9 BDSG, zulässig ist, und erst in einem weiteren zweiten Schritt die Zulässigkeit des einzelnen Abrufs von Bedeutung ist.[1888]
Hierbei enthält § 10 Abs. 1 S. 1 BDSG Kriterien zur Zulässigkeit und Angemessenheit des Abrufverfahrens, die vor Einrichtung zu prüfen sind, und zudem § 10 Abs. 2 BDSG verlangt, dass das Ergebnis dieser durchgeführten Interessenabwägung neben Anlass und Zweck der automatisierten Einrichtung, Datenempfänger, Art der Daten und den getroffenen Maßnahmen nach § 9 BDSG schriftlich festzulegen ist.[1889]
Damit ist ebenso eine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten gemäß § 4 d Abs. 5 BDSG verbunden.[1890]

---

landesdatenschutzrechtlichen Regelungen allein auf die Datenverarbeitung durch die jeweiligen Behörden abstellen, unabhängig vom Ort der Verarbeitung (§ 2 Hamburgisches Datenschutzgesetz, § 2 Niedersächsisches Datenschutzgesetz, § 2 Datenschutzgesetz Nordrhein-Westfalen, § 2 Landesdatenschutzgesetz Rheinland-Pfalz, §§ 2 Abs. 3, 3 Landesdatenschutzgesetz Schleswig-Holstein, § 2 Baden-Württembergisches Landesdatenschutzgesetz, § 2 Bayerisches Datenschutzgesetz, §§ 1 Abs. 2, 2 Berliner Datenschutzgesetz, § 1 Bremisches Datenschutzgesetz, § 3 Hessisches Datenschutzgesetz, § 2 Saarländisches Datenschutzgesetz, § 2 Thüringer Datenschutzgesetz, § 2 Sächsisches Datenschutzgesetz, § 2 Brandenburgisches Datenschutzgesetz, § 3 Datenschutzgesetz Sachsen-Anhalt, § 2 Landesdatenschutzgesetz Mecklenburg-Vorpommern). Artikel 8 Baden-Württembergisches Landesdatenschutzgesetz und Artikel 8 Bayerisches Datenschutzgesetz haben die Regelung des § 10 BDSG inhaltlich übernommen.
[1887] Siehe hierzu die Ausführungen oben S. 396 ff. Siehe aber ebenso die rechtspolitischen Überlegung zur Funktionsübertragung auf S. 429.
[1888] Siehe Ehmann in: Simitis, BDSG-Kommentar, § 10 BDSG Rn. 39.
[1889] Gola/Schomerus, BDSG, § 10 BDSG Rn. 14. Siehe hierzu auch Ehmann in: Simitis, BDSG-Kommentar, § 10 BDSG Rn. 85.
[1890] Gola/Schomerus, BDSG, § 10 BDSG Rn. 13. Es handelt sich jedoch nicht um ein formales Genehmigungsrecht des Datenschutzbeauftragten und damit nicht um eine Rechtmäßigkeitsvoraussetzung. Da auch in den Straf- und Bußgeldtatbeständen der §§ 43, 44 BDSG ein Verstoß hiergegen nicht erfasst ist, ist insoweit allein die Aufsichtsbehörde zuständig, um Beanstandungen auszusprechen (siehe hierzu im Gesamten Gola/Schomerus, BDSG, § 4d BDSG Rn. 15).

Dies bedeutet aber ebenfalls, dass mit der Einrichtung eines VPN, insoweit Schwierigkeiten verbunden sein können, wenn mehrere externe Stellen, wie etwa Tochterunternehmen, Zweigstellen oder Externe, zugriffsberechtigt sein sollen, da bereits im vorhinein und schriftlich für jeden einzelnen dieser Zugriffsberechtigten gemäß § 10 Abs. 2 Nr. 3 BDSG die Art der Daten, die übermittelt werden, sowie gemäß § 10 Abs. 2 Nr. 4 BDSG gegebenenfalls jeweils unterschiedliche technische oder organisatorische Maßnahmen festgelegt werden müssen, je nachdem ob sich bei den einzelnen Stellen Unterschiede im Datenschutzniveau ergeben.
Wird der Zugriff beispielsweise einem freien Mitarbeiter gewährt, der nicht in den Betrieb oder das Unternehmen eingegliedert ist, ergibt die Interessenabwägung gegebenenfalls, dass ihm andere Zugriffsrechte zu gewähren sind als beispielsweise einem Tochterunternehmen.
Die Pflicht zur Verschlüsselung im Verhältnis zwischen VPN-Auftraggeber und Betroffenem bleibt jedoch stets die gleiche, wobei nicht nur die Schlüssellänge entscheidend ist, sondern ebenso die Anforderungen an Sicherstellung von Authentizität und Integrität.[1891]

Es muss daher (entsprechend den Ausführungen zur Auftragsdatenverarbeitung)[1892] gelten, dass im Hinblick auf die Rechte des Betroffenen ebenso der Weg der Daten über das Internet in die Schutzmaßnahmen miteinzubeziehen ist. Denn dadurch kann die Unsicherheit des Internet überbrückt werden und diejenigen, die die Datenverarbeitung vornehmen behalten die für die Verwirklichung der Rechte des Betroffenen notwendige Einflussmöglichkeit über die Daten.

Hieraus wird ersichtlich, dass an die Planung eines VPN, welches mehreren und organisatorisch getrennten Personen Zugriffsrechte auf Daten gewähren soll, erhebliche Anforderungen zu stellen sind.
Es stellt zwar im Gesamten ein automatisiertes Verfahren, dar, hat aber im Einzelnen unterschiedliche Zulässigkeitsvoraussetzungen, die detailliert im

[1891] Siehe die Ausführungen zur Datenintegrität und den Authentifizierungsmöglichkeiten auf S. 408 ff. Zur Verschlüsselungspflicht siehe S. 412. Vgl. zu den Verschlüsselungsmöglichkeiten oben S. 39 ff. sowie zur Empfehlung der IETF Fn. 1082. Siehe zu den Voraussetzungen eines Software-VPN S. 53 ff. sowie zu den Nachteilen insbesondere Fn. 227.
[1892] Siehe die Ausführungen auf S. 427 ff.

Hinblick auf sämtliche zugriffsberechtigte Personen im Vorhinein geprüft werden müssen.[1893]
Die hierbei vorzunehmende Abwägung zwischen den Interessen von VPN-Auftraggeber und Dritten orientiert sich an den gleichen Voraussetzungen wie § 28 Abs. 1 Nr. 2 BDSG,[1894] allerdings mit der Besonderheit hat, dass gemäß § 10 Abs. 2 BDSG eine schriftliche Fixierung dieser Interessenabwägung im Vorhinein erfolgen muss.
Aus § 10 Abs. 2 Nr. 2 BDSG i.V.m. § 9 BDSG ergibt sich zudem, dass der Einsatz eines Gateway sowie die sorgfältige Auswahl des Providers Teil eines Sicherheitskonzepts ist, welches schriftlich zu dokumentieren ist.

bbb. Telekommunikationsdienst

Im Rahmen eines VPN gibt es nicht nur die gerade dargestellte Möglichkeit, Daten vom Server abzurufen, sondern ebenso zu (nutzer)eigenen Zwecken, Daten auf den Server zu übertragen. Folge dieser Abgrenzung ist, dass zwischen VPN-Auftraggeber und Nutzer ein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG bejaht und der VPN-Auftraggeber als Diensteanbieter gemäß § 3 Nr. 6 TKG eingestuft wurde. [1895] Es werden keine (eigenen) Inhalte seitens des VPN-Auftraggebers bereitgehalten, sondern er stellt vielmehr „nur“ eine Datenempfangsanlage gemäß § 3 Nr. 23 TKG bereit, auf welche der Nutzer eigenständig Daten übertragen kann.[1896] Bei dieser Möglichkeit steht daher die Transportfunktion im Vordergrund. Ein nutzereigener Zweck kann etwa die Übertragung der eigenen Daten zu Bestellzwecken sein. In diesem Falle sind keine Rechte Dritter betroffen. Es kommt aber ebenso die Möglichkeit des Online-Backup-Verfahrens in Betracht,[1897] so dass der Nutzer (beispielsweise das Tochterunternehmen) den Server zur Übertragung und zum Hosting eigener Daten oder Daten eines Betroffenen (beispielsweise Kunde des Tochterunternehmens) verwendet.

[1893] Zur Notwendigkeit abgestufter Zugriffsberechtigungen für die Angemessenheit der Einrichtung des Abrufverfahrens siehe Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 393.
[1894] Vgl. Schaffland/Wiltfang, BDSG, § 10 BDSG Rn. 4.
[1895] Siehe zur rechtlichen Einordnung als Telekommunikationsdienst die Ausführungen auf S. 312 ff. Zu den datenschutzrechtlichen Konsequenzen siehe S. 341 ff.
[1896] Siehe hierzu S. 312 ff.
[1897] Siehe zum Online-Backup S. 74 ff.

In datenschutzrechtlicher Hinsicht muss im Hinblick auf die Rechte des Betroffenen eine Auftragsdatenverarbeitung gemäß § 11 BDSG zwischen VPN-Auftraggeber und Nutzer, wie beispielsweise dem Tochterunternehmen, vereinbart werden. Sofern das Tochterunternehmen Einfluss auf die technischen und organisatorischen Maßnahmen nehmen kann und die Daten so verarbeitet werden, als würde das Tochterunternehmen diese Datenverarbeitung selbst vornehmen, ist der Betroffene optimal geschützt. In diesem Zusammenhang ist nochmals das Manko der Funktionsübertragung zu betonen:[1898] Zwar könnte gemäß § 28 Abs. 1 Nr. 2 BDSG durch die in einem VPN sichergestellten technischen und organisatorischen Maßnahmen eine Datenübermittlung zu Hostingzwecken gerechtfertigt sein. Es wären darüber hinaus ebenso die schutzwürdigen Interessen des Betroffenen ausreichend berücksichtigt, sofern die Datenverarbeitung auf dem Server des VPN-Auftraggebers nicht zu eigenen Zwecken erfolgt (in diesem Falle müsste zwangsläufig eine ausdrückliche Einwilligung des Betroffenen erfolgen).[1899] Dennoch erfordert der optimale Schutz der datenschutzrechtlichen Interessen des Betroffenen die Vereinbarung einer Auftragsdatenverarbeitung gemäß § 11 BDSG unter Berücksichtigung der Kontrollbefugnisse und Weisungsrechte.[1900]

Diese Forderung gilt ebenso aus dem folgenden Gesichtspunkt: Der VPN-Auftraggeber wäre im Falle einer Funktionsübertragung dem Dritten gegenüber weder zur Einhaltung des Fernmeldegeheimnisses gemäß § 88 TKG noch zur Vornahme von Sicherheitsmaßnahmen gemäß § 109 TKG verpflichtet.[1901] Betroffene, die nicht selbst oder unmittelbar an der Telekommunikation beteiligt sind, können keine Ansprüche aus dem TKG herleiten. Dieses richtet sich allein an die Beteiligten[1902] eines Telekommunikationsdienstes.

[1898] Siehe S. 429 ff.
[1899] Siehe S. 429 ff.
[1900] Siehe zu den Kontrollbefugnissen und Weisungsrechten Walz in: Simitis, BDSG-Kommentar, § 11 BDSG Rn. 40 ff. sowie zur Weisungsgebundenheit des Auftragnehmers Rn. 56 ff.
[1901] Auch der Server selbst, auf welchen die Daten übertragen werden, stellt im Übrigen eine Telekommunikationsanlage gemäß § 3 Nr. 23 TKG dar, da es sich hier um eine technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren kann, vgl. Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 2; Vgl auch Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 11; Haß in: Manssen, Kommentar Telekommunikations- und Multimediarecht, § 85 TKG(1998), Band 1, Rn. 11.
[1902] Nutzer gemäß § 3 Nr. 14 TKG oder Teilnehmer gemäß § 3 Nr. 20 TKG.

So hat § 88 TKG zwar drittschützenden Charakter, aber allein im Hinblick auf die Nutzer des Dienstes und nicht im Verhältnis zum Betroffenen.[1903] Die datenschutzrechtlichen Pflichten, die sich aus dem BDSG ergeben, sind also gegenüber einem Betroffenen klar von den Regelungen und Pflichten des TKG zu trennen. Der VPN-Auftraggeber wäre daher allenfalls im Verhältnis zu seinen Nutzern zur Wahrung des Fernmeldegeheimnisses gemäß § 88 TKG und zur Vornahme von Sicherheitsmaßnahmen gemäß § 109 TKG verpflichtet. Daher stellt § 88 TKG auch keine dem § 10 BDSG entsprechende Norm dar, die den Schutz eines Betroffenen „vor den Nutzern" bezwecken würde,[1904] wobei die unmittelbare Anwendung von § 10 BDSG hier allerdings ohnehin nicht in Betracht kommt. Denn für die Anwendbarkeit von § 10 BDSG ist das gezielte Bereithalten von Informationen zur Einsichtnahme notwendig,[1905] was beim Bereitstellen eines Servers, um dort Daten abzulegen zu können nicht der Fall ist.

Ein besonders wichtiger Punkt ist in diesem Zusammenhang allerdings, dass es gleichermaßen auf die tatsächlichen Umstände des „gelebten" Vertrages ankommt.[1906]

Bei der Auftragsdatenverarbeitung kommt es stets darauf an, wie konkret im Einzelfall der Auftrag ausgestaltet ist und welche Einflussrechte dem Auftraggeber noch verbleiben bzw. ob er seine Einflussrechte und die Verfügungsmacht als „Herr der Daten" verliert. [1907]

Zwar wird beim Datenhosting, die Datenverwaltung und die technische Verwaltung im Vordergrund stehen, so dass von einer

[1903] Büchner in: TKG-Kommentar, § 85 TKG Rn. 23; Vgl zum persönlichen Schutzbereich des § 88 TKG auch Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 19; siehe ebenso Zerres in: Scheurle/Mayen, TKG-Kommentar, § 85 TKG Rn. 20, der darlegt, dass der Schutzbereich von § 85 Abs. 1 TKG (a.F.) nicht nur zugunsten des „anrufenden" Telekommunikationsnutzers, sondern auch als eigenes Recht zugunsten des „Angerufenen" gilt. In diesem Sinne ebenso Klesczewski in: Berliner Kommentar zum TKG, § 88 TKG Rn. 10, der den personalen Anwendungsbereich zugunsten des „Anrufers" und des „Angerufenen" festlegt.

[1904] Gola/Schomerus, BDSG, § 10 BDSG Rn. 7.

[1905] Auernhammer, BDSG, § 3 BDSG Rn. 38. Siehe auch Auernhammer, BDSG, § 10 BDSG Rn. 2, wo ausgeführt wird, dass es sich beim Abruf um eine Form der Übermittlung handelt.

[1906] Siehe hierzu die Ausführungen auf S. 150 ff. Vgl. zum Widerspruch zwischen der praktischen Tätigkeit und der schriftlichen Vereinbarung im Arbeitsverhältnis Wedde, Telearbeit, S. 39 unter Verweis auf die Entscheidung des BAG v. 24.06.1992 AP Nr. 61 zu § 611 BGB Abhängigkeit.

[1907] Siehe zur Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung die Ausführungen auf S. 382. Siehe außerdem Gola/Schomerus, BDSG, § 11 BDSG Rn. 9; Wronka, RDV 2003, 132, 132. Vgl. ebenso Kramer/Herrmann, CR 2003, 938, 938; Evers/Keine, NJW 2003, 2726, 2727; Steding, BB 2001, 1693, 1698; Müthlein/Heck, Outsourcing, S. 34 ff.

Auftragsdatenverarbeitung grundsätzlich auszugehen ist.[1908] Es muss aber bei der Ausgestaltung einer Auftragsdatenverarbeitung nicht nur der konstitutive Charakter der Schriftform bei der Auftragsdatenverarbeitung berücksichtigt werden,[1909] sondern es müssen insbesondere die Einzelheiten der Kontrolle eindeutig geregelt sein und auch auf deren tatsächliche Durchführung geachtet werden. So müssen unter anderem die räumlichen, organisatorischen und personellen Maßnahmen zur Abgrenzung der Datenverarbeitung zu anderen Unternehmensbereichen geregelt sowie Regelungen zur Aufbewahrung und Vernichtung bzw. Löschung der Daten getroffen werden.[1910]

Hierzu muss als wesentlicher Bestandteil ebenso eine Vereinbarung über die Art und Weise der Datenübermittlung gehören. Gemäß § 11 Abs. 2 S. 2 BDSG muss zudem eine schriftliche Vereinbarung im Rahmen der Auftragsdatenverarbeitung getroffen werden, da anderenfalls die für eine Auftragsdatenverarbeitung erforderliche Verfügungsmacht über die Daten nicht gewährleistet ist.[1911]

Ist das Online-Backup-Verfahren derart ausgestaltet, dass letztendlich im tatsächlichen Sinne keine Einflussnahme mehr seitens des Nutzers ausgeübt werden kann, muss insgesamt von einer Funktionsübertragung ausgegangen werden. Dies kann entweder in Betracht kommen, wenn keine konkreten Regelungen zur Auftragsdatenverarbeitung vereinbart sind bzw. auf deren Einhaltung nicht geachtet wird und keine Kontrollen durchgeführt werden, oder aber der VPN-Auftraggeber die Daten des Betroffenen beispielsweise für eigene (Werbe)Zwecke verarbeitet.

Allein die (beabsichtigte) technische Übertragung der Datenverwaltung kann daher nicht das entscheidende Kriterium sein, um eine Auftragsdatenverarbeitung zu bejahen. Maßgeblich ist vielmehr, ob der VPN-Auftraggeber tatsächlich noch „Herr der Daten“ bleibt, was vorrangig davon abhängt, ob und inwieweit er die Einzelheiten der Auftragsdatenverarbeitung geregelt hat.

[1908] Vgl. hierzu auch Kramer/Herrmann, CR 2003, 938, 938, Müthlein/Heck, Outsourcing und Datenschutz, S. 34 ff.; Niedermeier/Schröcker, RDV 2001, 90, 92. Steding, BB 2001, 1693, 1699 ff.

[1909] Gola/Schomerus, BDSG; § 11 BDSG Rn. 17; Schaffland/Wiltfang, BDSG, § 11 BDSG Rn. 9a.

[1910] Vgl. im Einzelnen zu den Maßnahmen Gola/Schomerus, BDSG; § 11 BDSG Rn. 18.

[1911] Siehe zur „Hilfsfunktion“ der Auftragsdatenverarbeiters Walz in: Simitis, BDSG-Kommentar, § 11 BDSG Rn. 17.

Aus diesen Ausführungen wird ebenso das folgende Dilemma klar: Die Auftragsdatenverarbeitung gemäß § 11 BDSG kann letztendlich durch zulässige Datenübermittlungen im Sinne von § 28 Abs. 1 Nr. 2 BDSG sowohl in rechtlicher als auch in praktischer Sicht ausgehebelt werden. Denn für Datenübermittlungen und Datenverarbeitungen, die für eigene Geschäftszwecke des jeweiligen Auftraggebers erfolgen, wird keine ausdrückliche Einwilligung des Betroffenen verlangt. Dies könnte nur dann verhindert werden, wenn der Übermittlungstatbestand von der gesetzlichen Regelung des § 28 Abs. 1 BDSG ausgenommen wäre. Eine weitere Möglichkeit wäre eine ausdrückliche gesetzliche Klarstellung, dass das schutzwürdige Interesse des Betroffenen stets verletzt ist und gemäß § 28 Abs. 1 Nr. 2 BDSG überwiegt, sofern im Falle der Datenübertragung kein Auftragsdatenverarbeitungsvertrag gemäß § 11 BDSG geschlossen wird.

Der Schutz des Betroffenen wird daher bei einer Funktionsübertragung allein dadurch gesichert, dass der Datenverarbeiter bzw. der VPN-Auftraggeber diesem Falle dem Betroffenen gegenüber ebenso zur Einhaltung von Datenschutz verpflichtet ist.[1912]
Im Verhältnis zum Betroffenen wandelt sich der Begriff des Dritten dementsprechend.[1913] Beiden Fällen liegt der gleiche Sachverhalt zugrunde. Dennoch ist in dem einen Fall der VPN-Auftraggeber ein Dritter gemäß § 3 Abs. 8 BDSG. In dem anderen Fall scheidet der Drittbezug aufgrund Auftragsdatenverarbeitung gemäß § 11 BDSG aus.

3. Zwischenergebnis

Telearbeit ist aus datenschutzrechtlicher Sicht insgesamt nur zulässig, sofern die berechtigten Interessen des Betroffenen gemäß § 28 Abs. 1 Nr. 2 BDSG gewahrt sind. Insgesamt sollte hierbei die Durchführung von Telearbeit im häuslichen Bereich eines Arbeitnehmers im Hinblick auf die Verarbeitung personenbezogener oder sensitiver Daten nicht von vorneherein abgelehnt

[1912] Vgl. hierzu im Besonderen auch Gola/Schomerus, BDSG, § 27 BDSG Rn. 5.
[1913] Siehe zum Begriff des Dritten auch Gola/Schomerus, BDSG, § 3 BDSG Rn. 52; außerdem Gola/Schomerus, BDSG, § 11 BDSG Rn. 9.

werden,[1914] sondern auch beachtet werden, dass der Einsatz entsprechender Technik den Datenschutz der Betroffenen unterstützen kann. Dies kann gegebenenfalls dadurch erfolgen, dass im Wege des Application Service Providing Daten unmittelbar auf dem Server des VPN-Auftraggebers bearbeitet werden können.[1915]

Im Hinblick auf die Zulässigkeit von Telearbeit muss einschränkend gelten, dass Verschlüsselungen und Schutzmechanismen bei der Übertragung von personenbezogenen Daten Betroffener (wie sie moderne Verschlüsselungstechnologien bieten) eingesetzt werden müssen.
Bei Telearbeit ist im Übrigen eine Pflicht zur Verschlüsselung von Daten eindeutig zu normieren, soweit es sich um personenbezogene Daten von Betroffenen (also Kunden oder Mitarbeitern) handelt.
Dies ist Teil der erforderlichen organisatorischen und technischen Maßnahmen, die derjenige, der das VPN betreibt und Telearbeit anbietet, beachten muss.

Es können auch sensible Daten verarbeitet werden, insbesondere sofern es sich um reine Standortvernetzung handelt. Hierbei ist aber zu berücksichtigen, dass es unterschiedliche Verschlüsselungssysteme gibt, so dass es Pflicht des VPN-Auftragebers ist, diesbezüglich, die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um das bestmögliche Verschlüsselungssystem einzusetzen. Die Bedienung von Kryptographieprogrammen wird einfacher und der Stand der Technik entwickelt sich fort.[1916] Damit wachsen die Anforderungen an die Zulässigkeit von Telearbeit, so dass die Fortentwicklung der Technik gleichermaßen Einfluss auf die Zulässigkeit von Telearbeit hat.

Insgesamt ist daher im Hinblick auf die Rechte des Betroffenen zu berücksichtigen, ob und inwieweit bei einem VPN die Gefährdung der Daten des Betroffenen durch den Einsatz von Verschlüsselungstechniken stark eingeschränkt werden kann. Dies kann ebenso Bedeutung für die Frage haben, ob im Einzelfall eine Auftragsdatenverarbeitung vorliegt oder ob allein aufgrund

[1914] Siehe aber Hartig/Eiermann in: Roßnagel, Handbuch Datenschutzrecht, 6.5 Rn. 11.
[1915] Siehe auch Wedde, DuD 1998, 576, 578 zur datenschutzrechtlichen Gesamtverantwortlichkeit des Arbeitgebers.
[1916] Backu, ITRB 2003, 251, 253.

des Aspekts der unsicheren Datenübertragung über das Internet eine Auftragsdatenverarbeitung nicht mehr in Betracht kommen kann, da weder der Nutzer als datenverarbeitende Stelle (z.B. Tochterunternehmen) noch der der VPN-Auftraggeber, Einfluss auf den Gefahrenbereich nehmen kann und insoweit eine nicht mehr beherrschbare Verselbständigung der Daten bzw. des Datenflusses eingetreten ist. Denn wie oben ausgeführt, beinhaltet das Konzept der Auftragsdatenverarbeitung stets, dass der Auftraggeber noch „Herr der Daten" bleibt.
Daher müssen die Voraussetzungen der Auftragsdatenverarbeitung, und zwar ebenso im Hinblick auf die Datenübermittlung, konkret und schriftlich geregelt werden, wobei der VPN-Auftraggeber auch die faktische Möglichkeit haben muss, diese durchsetzen.

Die „Herrschaft über die Daten" kann im Übrigen nicht nur aufgrund von Online-Telearbeit konterkariert sein, sondern ebenso durch die Verarbeitung der Daten im heimischen Umfeld des Arbeitnehmers Der Einfluss des Arbeitgebers auf die Art und Weise der Datenverarbeitung ist in diesem Falle stark eingeschränkt. Bei der Ausgestaltung des „Wie" des heimischen Arbeitsplatzes im Rahmen der Telearbeit müssen folglich ebenso die Interessen des Betroffenen und dessen Recht auf informationelle Selbstbestimmung berücksichtigt werden.
Da dem Betroffenen im Regelfall nicht bekannt ist, ob „seine" Daten im häuslichen Umfeld eines Arbeitnehmers verarbeitet werden, kann er das informationelle Selbstbestimmungsrecht nicht im Rahmen eines eigenverantwortlichen Selbstdatenschutzes eigenständig ausüben. Dennoch ist derjenige, der die Daten des Betroffenen verarbeitet, zur verantwortungsbewussten Datenverarbeitung verpflichtet und muss die Interessen des Betroffenen berücksichtigen. Hier kann es zur Kollision zwischen den Arbeitnehmerrechten und den Interessen des Betroffenen kommen, so dass im Einzelfall geprüft werden muss, welches Interesse als höherrangig zu bewerten ist. Gelangt man aber zu dem Ergebnis, dass in den für den Schutz des Betroffenen notwendigen Maßnahmen gleichzeitig ein erheblicher Eingriff in die Persönlichkeitsrechte des Arbeitnehmers vorliegt, den dieser nicht durch eine freiwillige Einwilligung legitimiert hat, so muss Telearbeit im Zweifel unterbleiben. Dieser Gesichtspunkt spielt insbesondere im Hinblick

auf die Kontrollrechte des VPN-Auftraggebers bzw. Arbeitgebers am heimischen Arbeitsplatz des Arbeitnehmers eine große Rolle. Diese sind einerseits notwendig, um die Interessen des Betroffenen ausreichend zu schützen. Andererseits ist jedoch genau zu prüfen und abzuwägen, inwieweit deren Gestattung durch den Arbeitnehmer tatsächlich dessen Persönlichkeitsrecht berührt. Insbesondere ist zu berücksichtigen, inwieweit ein Verzicht des Arbeitnehmers auf sein Widerrufsrecht (bezüglich der Gestattung von Kontrollbesuchen in seiner Wohnung) ausgeschlossen sein könnte.
Dies muss stets Frage des Einzelfalls sein, da hierzu nur anhand der tatsächlichen Umstände und situationsbezogen eine Aussage getroffen werden kann.
Im Besonderen ist bei Telearbeit zu berücksichtigen, dass der VPN-Auftraggeber die gegenüber dem Betroffenen für die Einhaltung des Datenschutzes maßgebliche Person bleibt. Er kann diese Verpflichtungen nicht auf seine Mitarbeiter im häuslichen Bereich abwälzen. Zur Sicherstellung des Datenschutzes kann er allenfalls als organisatorische Maßnahme regelmäßige datenschutzrechtliche Schulungen anbieten und die Vorgabe erteilen, dass Daten verschlüsselt zu übertragen sind.
Im Hinblick auf den letzten Punkt kann der Arbeitgeber jedoch die Rechner der Mitarbeiter so ausstatten, dass diese die entsprechende Verschlüsselungssoftware bereits beinhalten. Hier könnten darüber hinaus Einstellungen in der Weise vorkonfiguriert sein, dass eine Verbindung automatisch zum Unternehmensnetz aufgebaut wird, wobei der VPN-Auftraggeber die zusätzliche Anweisung an seine Arbeitnehmer erteilen müsste, dass diese Konfigurationen nicht geändert werden dürfen. Die Optimallösung wäre es, sofern der VPN-Auftraggeber bzw. Arbeitgeber dem jeweiligen Nutzer hierfür einen separaten Rechner zur Verfügung stellt und ihn anweist, diesen keinen weiteren Mitbewohnern oder Familienmitgliedern zur Verfügung zu stellen.
Dies beinhaltet insgesamt aber, dass der Arbeitgeber sich den Einfluss auf die datenschutzrechtlichen Maßnahmen sichern muss, und zwar auch im Hinblick auf die datenschutzrechtlichen Kontrollrechte im heimischen Bereich. Ansonsten läge streng genommen eine Funktionsübertragung auf die Mitarbeiter vor, die diese als Arbeitnehmer natürlich nicht wahrnehmen können

und einen Eingriff in deren Persönlichkeitsrechte darstellen würde. Hier liegt also der merkwürdige (Neben)Effekt vor, dass Kontrollrechte im heimischen Bereich ebenfalls den Schutz des Arbeitnehmers sicherstellen können.
Die datenschutzrechtliche Verantwortung des VPN-Auftraggebers für die Sicherstellung entsprechender Maßnahmen zum Schutze personenbezogener Daten ist bei Telearbeit auch im Rahmen der Auftragsdatenverarbeitung gemäß § 11 BDSG zu berücksichtigen. . Dementsprechend muss der VPN-Auftraggeber streng auf die konkrete schriftliche Ausgestaltung der Auftragsdatenverarbeitung achten. Es darf keine Situation entstehen, die letztendlich die datenverarbeitende Stelle zum Verantwortlichen der Datenverarbeitung macht, oder in der sich der Betroffene aufgrund eines nicht mehr beherrschbaren Gefahrenbereichs (wie beispielsweise der Datenübertragung über das Internet) keinem Verantwortlichen mehr gegenübersieht, der für die sichere Datenweitergabe einsteht.

Für die Zulässigkeit der Funktionsübertragung gilt, dass der derjenige, der „outsourct“ entweder gemäß § 28 Abs. 1 Nr. 2 BDSG hierzu legitimiert sein muss oder aber die Einwilligung des Betroffenen gemäß § 4 a BDSG vorliegen muss. Hierbei gilt die rechtspolitische Erwägung, dass Funktionsübertragung stets (auch bei Übermittlung zu eigenen Geschäftszwecken des Auftraggebers) nur mit Einwilligung des Betroffenen zulässig sein sollte und ansonsten die strengen Regelungen der Auftragsdatenverarbeitung gemäß § 11 BDSG zur Anwendung kommen müssen.
Ob im Einzelfall allerdings Auftragsdatenverarbeitung oder eine Funktionsübertragung vorliegt, kann lediglich anhand der tatsächlichen Umstände sowie der Frage ermittelt werden, inwieweit seitens des Auftraggebers Beherrschbarkeit über die Daten gegeben ist.

Werden die Daten des Betroffenen innerhalb eines Abrufverfahrens zur Verfügung gestellt, so sind darüber hinaus stets die Voraussetzungen des § 10 BDSG zu beachten.

II. Zusatzdienst E-Mail

Zu prüfen sind ebenso die die datenschutzrechtlichen Interessen eines Betroffenen, dessen Daten als Inhalt einer E-Mail versendet werden. Hier zeigt sich wiederum, dass die Betrachtung des Mehrpersonenverhältnisses erforderlich ist und außerdem zwischen privater und dienstlicher Kommunikation zu trennen ist, da die Ausführungen des Personenverhältnisses „VPN-Auftraggeber/Nutzer" wie folgt Berücksichtigung finden müssen:

Bei privater E-Mail-Kommunikation darf der VPN-Auftraggeber bzw. Arbeitgeber keine eigene Protokollierung vornehmen, insbesondere den Inhalt nicht einsehen.[1917] § 88 TKG findet zwar nicht unmittelbar im Verhältnis zum Betroffenen Anwendung.[1918] Der Betroffene wird hier jedoch mittelbar dadurch geschützt, dass der VPN-Auftraggeber im Verhältnis zum Nutzer zur Wahrung des Fernmeldegeheimnisses gemäß § 88 TKG verpflichtet ist. Er muss den Nutzer diesbezüglich nicht zur Einhaltung von datenschutzrechtlichen Pflichten anhalten, da bei privater Kommunikation das Datenschutzrecht keine Anwendung findet.[1919]

Um Datenschutz im Hinblick auf die Interessen des Betroffenen aber optimal sicherzustellen, ist es ebenso in diesem Zusammenhang notwendig, dass der VPN-Auftraggeber als Arbeitgeber und Diensteanbieter gemäß § 3 Nr. 6 TKG dem jeweiligen Nutzer bzw. Mitarbeiter Verschlüsselungssoftware anbietet und ihn zur Verschlüsselung seiner privaten Kommunikation auffordert.[1920]

Bei geschäftlicher Kommunikation hat der VPN-Auftraggeber ebenso wenig Einsichtsrechte in den Inhalt der Kommunikation. Dies folgt daraus, dass der Nutzer (Arbeitnehmer) des E-Mail-Dienstes ansonsten in seinen

[1917] Siehe S. 362 ff., wo auch darauf hingewiesen wurde, dass der Arbeitgeber auch den E-Mail-Kopf nicht einsehen darf.
[1918] Vgl. hierzu insbesondere auch die Ausführungen auf S. 436. Vgl. außerdem Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 23; Vgl zum persönlichen Schutzbereich des § 88 TKG auch Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 19; siehe ebenso Zerres in: Scheurle/Mayen, TKG-Kommentar, § 85 TKG Rn. 20. In diesem Sinne ebenso Klesczewski in: Berliner Kommentar zum TKG, § 88 TKG Rn. 10, der den personalen Anwendungsbereich zugunsten des „Anrufers" und des „Angerufenen" festlegt.
[1919] Innerhalb des privaten Bereiches findet gemäß § 3 Abs. 2 Nr. 3 BDSG der Datenschutz keine Anwendung.
[1920] Siehe hierzu die Ausführungen auf S. 366 ff.

Persönlichkeitsrechten verletzt wäre.[1921] Dennoch obliegen dem VPN-Auftraggeber im Verhältnis zum Betroffenen erhöhte Schutzpflichten.
Bei geschäftlicher E-Mail-Kommunikation kommt aber ebenso eine Pflicht zur Verschlüsselung in Betracht, wie oben im Hinblick auf die Telearbeit bejaht worden ist. Sofern personenbezogene Daten Dritter über das Internet versendet werden, ist es in der täglichen Praxis üblich geworden, diese zu verschlüsseln.[1922] Hierfür sprechen die überwiegenden Interessen des Betroffenen gemäß § 28 Abs. 1 Nr. 2 BDSG. Auch beim Versenden per E-Mail handelt es sich entweder um ein Nutzen von Daten der Betroffenen gemäß § 3 Abs. 5 BDSG oder aber um ein Übermitteln gemäß § 3 Abs. 4 Nr. 3 BDSG, je nachdem ob der Empfänger Dritter gemäß § 3 Abs. 8 BDSG ist.[1923]

Zu berücksichtigen ist hierbei jedoch, dass die Verschlüsselungen in Bezug auf E-Mails, insbesondere PGP, noch nicht so weit gesichert ist, dass dies mit Verschlüsselungen wie IPSec vergleichbar ist.[1924] Daher muss im Einzelfall eine Übermittlung von personenbezogenen oder gar sensitiven Daten per E-Mail unterbleiben, sofern die überwiegenden Interessen des Betroffenen gemäß § 28 Abs. 1 Nr. 2 BDSG einer solchen Nutzung, etwa wegen Unsicherheit bei der Übertragung entgegenstehen. Es muss stets geprüft werden, ob nicht ein gesicherter Datenbankzugriff den Interessen des Betroffen besser Rechnung trägt als die Versendung seiner Daten per E-Mail.
Auch muss zur Sicherstellung der Zugriffssicherheit auf digitale Signaturen zurückgegriffen werden.[1925]

[1921] Siehe hierzu die Ausführungen auf S. 361 ff. Siehe aber zu den Persönlichkeitsrechten des E-Mail-Kommunikationspartners S. 374 ff.
[1922] Siehe auch Schaar in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 401 mit dem Hinweis, dass sich die Datenschutzbeauftragen des Bundes und der Länder auf die Verschlüsselungssoftware PGP verständigt haben, um damit ihren E-Mail-Austausch zu sichern.
[1923] Siehe hierzu die obigen Ausführungen auf S. 385 ff. Vgl. auch Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2. Rn. 70 mit dem Anmerkung, dass die Datenweitergabe innerhalb der verantwortlichen Stelle unter den Begriff der Nutzung gemäß § 3 Abs. 5 BDSG fällt.
[1924] Vgl. auch Voss, Das große PC & Internet Lexikon 2007, „OpenPGP“ S. 588, der auf die Sicherheitslücken von PGP gerade aufgrund seines Open Source Status verweist.
[1925] Zu der Pflicht zur Verschlüsselung von E-Mail-Kommunikation siehe Backu, ITRB 2003, S. 251 ff. (insbesondere auch S. 253). Backu (aaO) führt aus, dass es sich zum einen bei §§ 28, 29 BDSG um Schutzgesetze im Sinne von § 823 Abs. 2 BGB handelt. Vgl. außerdem die weiteren Ausführungen auf S. 412, insbesondere die weiteren Verweise in Fn. 1784.

C. Nutzer - Betroffener

Ein besonderes Problem bei Telearbeit besteht ebenso darin, inwiefern der jeweilige Nutzer gegenüber dem Betroffenen datenschutzrechtlich verpflichtet ist. Hierbei kann als Nutzer aber lediglich der Externe, die Zweigstelle oder das Tochterunternehmen in Betracht kommen, da dem Arbeitnehmer keine eigenen datenschutzrechtlichen Pflichten gegenüber einem Betroffenen obliegen können.[1926]

I. Teledienst und Abrufverfahren

Nutzer, wie Externe, Zweigstellen oder Tochterunternehmen, kommen mit Daten eines Betroffenen in Berührung, sofern dessen Daten innerhalb des VPN im Wege der Telearbeit übertragen werden.[1927]
Datenschutz bezüglich Telearbeit ist lediglich im Hinblick auf Nutzer zu prüfen, die im Verhältnis zum Betroffenen Dritte gemäß § 3 Abs. 8 BDSG darstellen. Ansonsten kommen keine eigenständigen datenschutzrechtlichen Pflichten der Nutzer gegenüber dem Betroffenen in Betracht. Der VPN-Auftraggeber muss in diesem Fall seine Mitarbeiter vielmehr auf das Datenschutzgeheimnis gemäß § 5 BDSG verpflichten (oder auf die Erfüllung der Voraussetzungen gemäß § 11 BDSG achten), und den Nutzern obliegen keine eigenverantwortlichen datenschutzrechtlichen Pflichten im Verhältnis zum Betroffenen.[1928]

Sofern es sich aber um inhaltsbezogene Kommunikation innerhalb eines VPN handelt, und damit ein Abrufverfahren gemäß § 10 BDSG in Betracht kommt,[1929] muss das externe[1930] Unternehmen nach §§ 10 Abs. 1 S. 2, 10 Abs. 4 S. 1, 28 Abs. 1 Nr. 2 BDSG selbständig prüfen, ob der einzelne Abruf zulässig ist.

[1926] Vgl. hierzu auch Wedde, Telearbeit, S. S. 133 mit dem Hinweis, dass der Arbeitgeber für die Einhaltung des Datenschutzes verantwortlich ist.
[1927] Siehe hierzu die obigen Ausführungen zur Telearbeit S. 381 ff.
[1928] Siehe Wedde, Telearbeit, S. 130 zur Verpflichtung auf das Datengeheimnis gemäß § 5 BDSG.
[1929] Zur Anwendbarkeit von § 10 BDSG siehe oben S. 430.
[1930] § 10 BDSG kommt nicht zur Anwendung, wenn die Daten nur innerhalb einer speichernden Stelle zum Abruf bereitgestellt werden, da Abrufverfahren gemäß § 10 BDSG eine Übermittlung (§ 3 Abs. 5 Nr. 3 BDSG) personenbezogener Daten voraussetzen (vgl. Schaar in: Roßnagel, Handbuch der Multimedia-Rechte, § 4 TDDSG Rn. 315). Siehe ebenso Ehmann in: Simitis, BDSG-Kommentar, § 10 BDSG Rn. 8.

Dies bedeutet, dass der Betroffene dadurch hinsichtlich der Gewährleistung seines Datenschutzes eine zweite Kontrollinstanz hat. Denn auch hier muss eine Interessenabwägung durch die Zweigstelle, das Tochterunternehmen oder den Externen, wie beispielsweise Lieferanten oder freien Mitarbeiter,[1931] vorgenommen werden. Von diesen Personen ist ebenfalls zu prüfen, ob die technischen Maßnahmen(beispielsweise Zugriffsberechtigungen oder Verschlüsselungen) ausreichend sind und ob der Zugriff auf (bestimmte) Daten des Betroffenen im Sinne eines effektiven Datenschutzes ausgeschlossen ist.[1932] Nur wenn diese Voraussetzungen vorliegen, ist der Zugriff im Einzelfall berechtigt.

Von dieser Verpflichtung der abrufenden Stelle bleiben dennoch die oben festgestellten Verpflichtungen des VPN-Auftraggebers aus § 28 Abs. 1 Nr. 2 BDSG unberührt.[1933] Denn auch die verantwortliche Stelle muss einschreiten, wenn sie einen Anlass zur Annahme hat, dass der Dritte unzulässig abruft oder gegen datenschutzrechtliche Verpflichtungen verstößt.[1934] Der VPN-Auftraggeber muss damit ebenfalls eine Interessenabwägung im Hinblick auf die Datenübermittlung vornehmen.
Für die Anwendbarkeit von § 10 BDSG ist im Übrigen das gezielte Bereithalten von Informationen zur Einsichtnahme notwendig,[1935] wobei die entscheidende Aktivität vom Empfänger der Daten ausgehen muss.[1936]
Für eine „gleichberechtigte“ Standortverbindung innerhalb eines VPN bedeutet dies, dass jeder Standort sowohl speichernde Stelle und abrufende Stelle gemäß § 10 BDSG und § 28 Abs. 1 Nr. 2 BDSG ist. Denn in diesem Fall liegt an jedem Standort ein Abrufverfahren im Sinne von § 10 BDSG vor, da eine Weitergabe an Dritte im Rahmen einer „Selbstbedienung“ erfolgt.[1937]

[1931] Siehe jedoch zum Status der freien Mitarbeiter unbedingt die Ausführungen von Trümmer in: Däubler/Kittner/Klebe, BetrVG, § 5 BetrVG Rn. 57 ff. Es ist insbesondere entscheidend, wie das Vertragsverhältnis tatsächlich ausgestaltet und durchgeführt wird. Daher kann im Einzelfall ein Arbeitsverhältnis vorliegen, auch wenn kein Arbeitsvertrag im formalen Sinne abgeschlossen wurde!
[1932] Siehe hierzu etwa oben Fn. 1864.
[1933] Siehe S. 430 ff.
[1934] Vgl. hierzu auch Gola/Schomerus, BDSG, § 10 BDSG Rn. 10.
[1935] Auernhammer, BDSG, § 3 BDSG Rn. 38. Siehe auch Auernhammer, BDSG, § 10 BDSG Rn. 2, wo ausgeführt wird, dass es sich beim Abruf um eine Form der Übermittlung handelt.
[1936] Dammann in: Simitis, BDSG-Kommentar, § 3 BDSG Rn. 152.
[1937] Siehe hierzu Gola/Schomerus, BDSG, § 10 BDSG Rn. 5.

Sofern ansonsten aus Sicherheitsgründen lediglich von den Clients bzw. Tochterunternehmen, Zweigstellen oder Externen ein Verbindungsaufbau zu einem Server möglich ist,[1938] oder nur über diesen Server die gegenseitige Kommunikation erlaubt ist (wie etwa beim Software-VPN), dann kommt auf den ersten Blick eine „Selbstbedienung“ bezüglich der Daten nur im Hinblick auf diese „Außenstellen“ in Betracht, aber nicht im Hinblick auf den jeweiligen zentralen Standort.
Die Nutzer an diesem Standort können sich nicht frei entscheiden, zu einem Rechner eine Verbindung aufzubauen und dort Daten abzurufen.[1939]
Sind jedoch, wie etwa im obigen Beispiel,[1940] mehrere Standorte mittels eines Gateway ausgerüstet oder haben gegebenenfalls mehrere Rechner bei einem Software-VPN eine Benutzerverwaltung und VPN-Software installiert, die Voraussetzung für den VPN-Zugriff ist, dann liegt ein gegenseitiger Abruf von Daten zwischen diesen Stellen in Form einer „Selbstbedienung“ vor.

Fraglich ist allerdings, ob § 10 BDSG allein auf eine solche Auslegung begrenzt bleiben sollte. Denn zu berücksichtigen ist, dass ein bidirektionaler Datenaustausch stets möglich ist, sofern die Verbindung aufgebaut bzw. initiiert worden ist.[1941] Eine Selbstbedienung im Hinblick auf die Daten könnte dann in Betracht kommen, wenn beispielsweise ein so genannter Lockruf[1942] getätigt wird und wenn im Rahmen einer bestehenden Verbindung ein eigenständiger Zugriff auf die Daten am Nutzerstandort durch die Firmenzentrale gewährt wird.

Daher kann für die Anwendbarkeit des § 10 BDSG nicht nur entscheidend sein, wer die Verbindung aufbaut, sondern es muss insgesamt entscheidend sein, ob ein Nutzer auf Daten eines anderen Servers freien Zugriff nehmen und diese nach Belieben abrufen kann, unabhängig davon, wie der Verbindungsaufbau zustande gekommen ist.

[1938] Siehe hierzu S. 47/53.
[1939] Vgl. S. 55, wo ausgeführt ist, dass aus Sicherheitsgründen ein Verbindungsaufbau nur in Richtung der Firmenzentrale erfolgen kann.
[1940] Siehe das Beispiel auf S. 44, in welchem sowohl das Tochterunternehmen als auch die Unternehmenszentrale mit einem Gateway ausgerüstet sind.
[1941] Siehe Fn. 212.
[1942] Siehe zum von T-Online angebotenen Lockrufverfahren Fn. 212.

II. Telekommunikationsdienst

Im Verhältnis zwischen VPN-Auftraggeber und Nutzer (Externer, Zweigstelle und Tochterunternehmen) wurde bei gemeinsamer Zweckverfolgung die Anwendbarkeit von §§ 91 ff. TKG abgelehnt, da kein geschäftsmäßiges Handelt gemäß § 3 Nr. 10 TKG vorliegt.[1943] Insoweit wurde ebenso die Feststellung getroffen, dass es sich bei dem Nutzer nicht um einen Dritten handelt. Gibt beispielsweise der VPN-Auftraggeber Daten eines Kunden an das Tochterunternehmen zum Zwecke der Bereitstellung weiterer Leistungen und gemeinsamer Bearbeitung eines Auftrages weiter, bilden der VPN-Auftraggeber und der Nutzer (Tochterunternehmen) eine Kommunikationseinheit und die Eigenschaft als „Dritter“ scheidet aus.
Im Verhältnis zum Betroffenen wandelt sich dieser Begriff nun allerdings. Werden seine Daten zur Bearbeitung des Auftrags an das Tochterunternehmen weitergegeben, liegt aus seiner Sicht eine Funktionsübertragung und die Eigenschaft des Dritten vor. Das Tochterunternehmen steht unter Berücksichtigung von § 3 Abs. 8 BDSG außerhalb der verantwortlichen Stelle.

Dies hat zur Folge, dass die Weitergabe der Daten des Betroffenen eine Übermittlung gemäß § 3 Abs. 4 Nr. 3 BDSG für (auch) eigene Zwecke des Nutzers darstellt. Damit scheidet die Anwendbarkeit des § 28 Abs. 1 Nr. 2 BDSG aus und der Betroffene muss einer solchen Übermittlung gemäß § 4a BDSG ausdrücklich einwilligen.[1944]

[1943] Siehe S. 312 ff. sowie S. 337 ff., S. 338.
[1944] Siehe hierzu insbesondere S. 429 ff. und Fn. 1874 unter Verweis auf die Ausführungen von Däubler und Simitis. Es gibt im Rahmen der Datenverarbeitung kein Konzernprivileg, sofern bei der Verarbeitung ebenso eigene Geschäftszwecke verfolgt werden (Däubler, Gläserne Belegschaften?, Rn. 450 ff.; Simitis in: Simitis, BDSG-Kommentar, § 2 BDSG Rn. 150 ff.).

D. Provider – Betroffener

Im Rahmen des in diesem Teil untersuchten Arbeits- und Nutzungsverhältnisses interessiert gleichermaßen die Fragestellung, ob den Provider unmittelbare datenschutzrechtliche Pflichten gegenüber einer Person treffen, mit der er selbst in keinem Vertragsverhältnis steht.
Für die Pflichten des Providers gegenüber einem solchen Betroffenen ist im besonderen Maße die VPN-Variante relevant, bei welcher der Provider das Management des Gateways im Sinne einer Funktionsherrschaft übernimmt und ebenso für die Verschlüsselung Sorge trägt. Diese Variante wurde als Komplettmanagement des Gateway bezeichnet.[1945] Bei dieser VPN-Variante ist der Provider für die Sicherheitsstrategie des VPN verantwortlich.

Wer geschäftsmäßig Telekommunikationsdienste erbringt, hat zwar gemäß § 109 Abs. 1 TKG angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses zu treffen.[1946]
Diese Verpflichtung betrifft den Provider allerdings nur im Verhältnis zum Teilnehmer oder Nutzer des Dienstes, da § 88 TKG nur im Verhältnis zum Nutzer drittschützende Wirkung hat.[1947] Auch etwaige Schadensersatzansprüche gemäß § 44 TKG kann der Betroffene nicht unmittelbar gegen den Provider geltend machen.[1948]

[1945] Siehe S. 49 sowie die rechtlichen Ausführungen zur Funktionsherrschaft auf S. 154 ff.
[1946] Gola/Klug, Grundzüge des Datenschutzrechts, S. 199; zur Einholung einer Verpflichtungserklärung siehe auch Königshofen, RDV 1997, 97, 99.
[1947] Siehe S. 436. Vgl. auch Büchner in: TKG-Kommentar (2. Auflage), § 85 TKG Rn. 23; Vgl zum persönlichen Schutzbereich des § 88 TKG auch Bock in: TKG-Kommentar (3. Auflage), § 88 TKG Rn. 19; siehe ebenso Zerres in: Scheurle/Mayen, TKG-Kommentar, § 85 TKG Rn. 20. In diesem Sinne ebenso Klesczewski in: Berliner Kommentar zum TKG, § 88 TKG Rn. 10, der den personalen Anwendungsbereich zugunsten des „Anrufers" und des „Angerufenen" festlegt.
[1948] § 44 S. 3 TKG präzisiert nunmehr im Übrigen den Kreis der Anspruchsberechtigten entsprechend den Regelungen im novellierten UWG (siehe Begründung zum TKG-E, S. 98; zum novellierten UWG vgl. außerdem Fn. 1058). Die Klagebefugnis des § 13 UWG steht den Geschädigten nicht per se zu, sondern allenfalls den Verbraucherverbänden, Industrie- und Handelskammern oder Wettbewerbern (vgl. auch Anmerkung Eckhardt zu BGH, CR 2004, 445, 451, der darauf verweist, dass der Verbraucher als Schutzobjekt anerkannt ist, ihm aber kein eigenes Klagerecht zusteht). Siehe in diesem Zusammenhang aber auch Kloepfer in: Holznagel/Nelles/Sokol, TKÜV, S. 108 ff. zu den Gefährdungen der Privatsphäre durch die TKÜV und durch deutsche Behörden.

Der Betroffene, wird also durch das Fernmeldegeheimnis nicht unmittelbar als Beteiligter der Kommunikation geschützt, da er nicht selbst kommuniziert.[1949] Aber dadurch, dass der Provider gegenüber dem Nutzer und dem Teilnehmer als Diensteanbieter gemäß §§ 3 Nr. 6, 109 TKG zum Schutze des Fernmeldegeheimnisses verpflichtet ist, erstreckt sich der Schutz zwangsläufig ebenso (mittelbar) auf die Daten des Betroffenen.

Hiervon zu unterscheiden ist jedoch die Tatsache, dass der Provider nicht nur die Funktionsherrschaft über den Gateway ausüben kann, wenn er das Komplettmanagement des Gateways übernimmt.[1950] Es kann darüber hinaus ebenso eine Funktionsübertragung bezüglich der auf dem Gateway stattfindenden Datenverarbeitung vorliegen.[1951]

Im Verhältnis zwischen VPN-Auftraggeber und Betroffenen ist bereits eine Pflicht zur Verschlüsselung bei der Verarbeitung personenbezogener Daten festgestellt worden.[1952] Übernimmt der Provider nun auf dem Gateway die selbständige Verschlüsselung und Entschlüsselung der Daten, ohne im Sinne einer weisungsgebundenen Tätigkeit an Vorgaben des VPN-Auftraggebers gebunden zu sein, so hat nicht nur der VPN-Auftraggeber die Regelungen des § 28 Abs. 1 Nr. 2 BDSG bei der Funktionsübertragung zu beachten, sondern der Provider ist ebenso selbständig für den Datenschutz verantwortlich und muss die Interessen des Betroffenen gemäß § 28 Abs. 1 Nr. 2 BDSG berücksichtigen.[1953] Hier stellt sich die Frage, ob der Provider durch diese Tätigkeit die Daten des Betroffenen ebenso für eigene Geschäftszwecke (und nicht ausschließlich für die Geschäftszwecke des VPN-Auftraggebers) nutzt, so dass in diesem Falle die Verarbeitung ausschließlich mit Einwilligung des Betroffenen gemäß § 4a BDSG stattfinden dürfte. Ein solcher eigener Geschäftszweck, der über den Zweck der Erfüllung seiner vertraglichen Pflichten gegenüber dem VPN-Auftraggeber hinausgeht, ist jedoch nicht feststellbar.

Das vorrangige Problem liegt daher wiederum bei den eigentlichen Aufgaben

---

[1949] Vgl. auch Büchner in: TKG-Kommentar (2. Auflage), § 40 TKG Rn. 4 (in der neuen Auflage finden sich hierzu keine Ausführungen).

[1950] Siehe die rechtlichen Ausführungen zur Funktionsherrschaft auf S. 154 ff.

[1951] Siehe zur Abgrenzung zwischen Funktionsübertragung und Auftragsdatenverarbeitung S. 382 ff.

[1952] Siehe S. 412.

[1953] Vgl. Gola/Schomerus, BDSG, § 27 BDSG Rn. 5 zur Anwendbarkeit des § 28 Abs. 1 Nr. 2 BDSG sowohl für denjenigen, der die Funktion auslagert, als auch für denjenigen, der die Funktion wahrnimmt.

des Providers und der Abgrenzung zwischen Funktionsübertragung und Auftragsdatenverarbeitung. Erhält der Provider „freie Hand“ über die entsprechenden Maßnahmen, dann ist er weisungsunabhängig und kein Auftragsdatenverarbeiter gemäß § 11 BDSG.[1954] Er muss gemäß § 9 BDSG die erforderlichen Maßnahmen treffen, für die Schlüsselvernichtung Sorge tragen[1955] und bei der Datenweiterleitung[1956] vom Gateway in das lokale Netzwerk des VPN-Auftraggebers ebenso beachten, dass effektive Datenverschlüsselung stattfindet. Insoweit besteht ein Anspruch des Betroffenen.[1957]

Aber auch hier muss am konkreten Sachverhalt geprüft werden, inwieweit dem VPN-Auftraggeber noch eine Einflussnahme verbleibt, so dass letzterer unter Umständen „Herr der Daten“ bleibt. Da die Aufgabe des Providers nicht nur darin besteht, für die Einsatzbereitschaft seines Systems Sorge zu tragen, sondern er ebenso die Verschlüsselung, Entschlüsselung, gegebenenfalls die Benutzerauthentifizierung und die Datenweiterleitung, als „eine gesamte Aufgabe“,[1958] vornimmt, könnte dies über die weisungsabhängige technische Datenverarbeitung hinausgehen.[1959]

Der Provider kann zwar nicht selbständig Daten des Betroffenen erheben und ihm steht keine Entscheidungsbefugnis bezüglich der Auswahl der Daten zu, aber ihm verbleiben unter Umständen eigene Entscheidungsbefugnisse hinsichtlich des „Wie“ der Datenverarbeitung, bezüglich derer er selbständig „ohne Richtschnur“ des VPN-Auftraggebers handelt.[1960]

Der Provider nutzt die Daten des Betroffenen gemäß § 3 Abs. 5 BDSG nutzt, in dem er sie entschlüsselt,[1961] und anschließend weiterleitet bzw. an den VPN-Auftraggeber gemäß § 3 Abs. 4 Nr. 3 BDSG übermittelt.[1962] Damit stehen ihm

---

[1954] Vgl. hierzu die Ausführungen zum zwangsweisen Tunneling auf S. 284 ff.

[1955] Vgl. zum Erfordernis der Schlüsselvernichtung nach jedem Übertragungsvorgang S. 243 ff.

[1956] Siehe das Angebot von T-Online „Secure-VPN-Benutzerhandbuch“, S. 216 (mit dem Hinweis, dass auf dem Gateway die Entschlüsselung stattfindet und die Weitersendung ins lokale Netzwerk) sowie S. 239 ff.

[1957] Siehe zur Verschlüsselungspflicht S. 412.

[1958] Vgl. auch Geis, Recht im eCommerce, S. 74, der eine Funktionsübertragung dann annimmt, wenn die Aufgabe zur selbständigen Erledigung übertragen wird.

[1959] Vgl. hierzu auch Müthlein/Heck, Outsourcing und Datenschutz, S. 34 ff.; Niedermeier/Schröcker, RDV 2001, 90, 92.

[1960] Vgl. Kramer/Herrmann, CR 2003, 938, 939; Wächter, CR 1991, 333, 334.

[1961] Vgl. zum Nutzen auch Gola/Schomerus, BDSG, § 3 BDSG Rn. 41/42, wobei darunter auch die zielgerichtete Kenntnisnahme fällt.

[1962] Problematisch ist, ob im Hinblick auf die kurzzeitige Speicherung der Daten auf dem Gateway ein Speichern gemäß § 3 Abs. 4 Nr. 1 BDSG unterstellt werden kann (vgl. auch

eigene Entscheidungsbefugnisse zu, die für den Betroffenen datenschutzrechtlich nicht minder relevant sind als wenn der Provider eigenständig über die Auswahl der personenbezogenen Daten entscheiden könnte..

Auch wenn die Daten ausschließlich seitens des VPN-Auftraggebers erhoben und von diesem dem Provider zur Verfügung gestellt werden, was für eine Auftragsdatenverarbeitung gemäß § 11 Abs. 1 BDSG spricht,[1963] fällt die fehlende Einflussnahmemöglichkeit des VPN-Auftraggebers auf einen Teilbereich der Datenverarbeitung erheblich ins Gewicht. Daher kann ebenso eine Funktionsübertragung in Betracht kommen, sofern der VPN-Auftraggeber keine konkreten Vorgaben bezüglich der Datenverarbeitung gibt, sondern das „Wie" der Nutzung und Übermittlung allein die Hand des Providers legt. Er hat insoweit einen eigenen, originären Ermessensspielraum.[1964]

Provider, die ihre Angebote des Komplettmanagement einer breiten Masse unterbreiten, müssen daher besonderes Augenmerk darauf legen, dass die Betreuung der Funktionen auf Gateway und die Übernahme des Sicherheitsmanagements im Einzelfall nicht im Sinne einer Funktionsübertragung ausgelegt werden kann. Dies empfiehlt sich bereits aus strafrechtlichen Gesichtspunkten, da die Offenbarung eines Geheimnisses an einen nicht weisungsgebundenen Outsourcing-Partner unter Umständen ein Geheimnisverrat gemäß § 203 StGB darstellen kann. Wird beispielsweise das Gatewaymanagement in der Versicherungs- oder Gesundheitsbranche eingesetzt, so liegt hier ein besonderes Vertrauensverhältnis gemäß § 203 StGB vor. § 203 StGB erfasst zwar nicht alle Berufsgruppen und nicht alle Geheimnisse, sondern nur solche, die denn Verpflichteten in ihrer spezifisch beruflichen Eigenschaft anvertraut oder in sonstiger Weise bekannt geworden sind.[1965] § 203 Abs. 1 StGB enthält dennoch eine Verschwiegenheitspflicht für Angehörige solcher Berufsgruppen, denen sich der Einzelne in bestimmten Situationen anvertrauen muss. Von besonderer volkswirtschaftlicher Bedeutung

---

Gola/Schomerus, BDSG, § 3 BDSG Rn. 28; Schild in: Roßnagel, Handbuch Datenschutzrecht, 4.2 Rn. 56).

[1963] Vgl. Niedermeier/Schröcker, RDV 2001, 90, 93.

[1964] Vgl. Niedermeier/Schröcker, RDV 2001, 90, 93.

[1965] Vgl. Hoenike/Hülsdunk, MMR 2004, 788, 788, insbesondere auch S. 792, wo dargestellt wird, dass sich die momentane Rechtsunsicherheit dadurch minimieren lässt, indem zu den notwendigen Voraussetzungen nach Maßgabe des § 11 BDSG weitere Maßnahmen zum Schutz der Geheimnisse getroffen werden.

sind dabei die Unternehmen der privaten Kranken-, Unfall oder Lebensversicherung.[1966]

Auch dieser Gesichtspunkt spricht im Übrigen dafür, die Funktionsübertragung insgesamt als Möglichkeit der Datenverarbeitung abzulehnen und stattdessen eine Auftragsdatenverarbeitung gemäß § 11 BDSG zugrunde zu legen.[1967] Dementsprechend muss hier ein schriftlicher Auftragsdatenverarbeitung vereinbart werden, der konkret die Befugnisse des Providers und die Rechte des VPN-Auftraggebers festlegt.[1968] Allerdings besteht auch hier das Problem der „gelebten" Vertragsumstände.[1969] Der VPN-Auftraggeber wird praktisch nicht in der Lage sein, Kontroll- und Weisungsrechte auszuüben. Insbesondere wird ein Provider kein Interesse daran haben, ihm Zugangsrechte zu seinen Serverräumen einzuräumen (vgl. hierzu § 11 Abs. 2 S. 4 BDSG und Nr. 6 der Anlage zu § 9 BDSG). Dieses Problem kann man in rechtlicher Hinsicht nur dadurch auflösen, in dem man unterstellt, dass der Provider keinen Einblick in personenbezogene Daten des Betroffenen hat, da auf den vom ihm betreuten Systemen Daten stets nur verschlüsselt vorliegen. Folgt man jedoch der in dieser Arbeit vertretenen Auffassung, dass auch eine solche faktische Anonymität den Personenbezug nicht beseitigt,[1970] wäre stets der Abschluss eines Auftragsdatenverarbeitungsvertrages erforderlich.

Insgesamt zeigt sich, dass von Funktionsherrschaft über ein System die Datenverarbeitung auf dem System zu trennen ist.[1971] Funktionsherrschaft bedeutet nicht gleichzeitig Funktionsübertragung, sondern es kann ebenso eine Auftragsdatenverarbeitung gemäß § 11 BDSG vorliegen. Dies gilt ebenso, wenn der VPN-Auftraggeber das Systemmanagement in den Räumlichkeiten des VPN-Auftraggebers übernimmt. Auch in dieser Fallgestaltung kann (je nachdem, inwieweit dem Provider eigene Entscheidungsbefugnisse eingeräumt werden) eine Funktionsübertragung vorliegen. Anknüpfungspunkt für die

[1966] Siehe hierzu Hoenike/Hülsdunk, MMR 2004, 788, 788.
[1967] Siehe zu den rechtspolitischen Erwägungen bezüglich der Ablehnung einer Funktionsübertragung S. 429 ff.
[1968] Siehe hierzu die Ausführungen auf S. 437 ff.
[1969] Siehe hierzu den Verweis in der vorherigen Fußnote sowie die Ausführungen auf S. 150 ff.
[1970] Siehe S. 106 ff., insbesondere S. 109. Vgl. ebenso die Ausführungen auf S. 215 ff.
[1971] Siehe zur Funktionsherrschaft die Ausführungen in dem Personenverhältnis „Provider/VPN-Auftraggeber" S. 149 ff., insbesondere auch S. 152 ff., S. 154 ff.

Funktionsherrschaft über ein System muss die „tatsächliche Kontrollausübung“ anhand der Fragestellung sein, in welchem räumlichen Machtbereich sich das System befindet bzw. in wessen Netzwerk dieses integriert ist. Für die Auftragsdatenverarbeitung ist hingegen gesetzlich (gerade) geregelt, dass die Daten dem tatsächlichen Einfluss- und räumlichen Machtbereich des Auftraggebers entzogen sein können, was jedoch durch Weisungsrechte und jederzeitige Kontrollbesuche „kompensiert“ wird.

Der VPN-Auftraggeber muss folglich ebenso die Beziehung zwischen Provider und Betroffenen berücksichtigen. Auch aus diesem Grunde ist daher eine rechtliche Gesamtbewertung sämtlicher vertraglicher Beziehungen in einem VPN erforderlich.

5. Abschnitt
Zusammenfassung

Die Relevanz des Mehrpersonenverhältnisses (unter I.) und der Technik (unter II.) für eine datenschutzrechtliche Prüfung lässt sich anhand des Beispiels VPN wie folgt zusammenfassen:

I. Relevanz des Mehrpersonenverhältnisses:

1)
Das in dieser Arbeit zugrunde gelegte Verständnis eines Online-Dienstes als wirtschaftliche Tätigkeit im Internet führt zur Unterteilung des VPN in mehrere Dienstleistungen und unterschiedliche Personenverhältnisse.
Eine solche dienstorientierte Betrachtungsweise im Mehrpersonenverhältnis (die nicht vorrangig funktional zwischen Transport- und Inhaltsebene trennt) erlaubt zum einen eine umfassende Abgrenzung der rechtlichen Pflichten der unterschiedlichen Beteiligten. Zum anderen kann dadurch beurteilt werden, inwieweit sich die für ein Personenverhältnis festgestellten datenschutzrechtlichen Pflichten und Bedingungen unmittelbar in den weiteren beteiligten Personenverhältnissen des Online-Dienstes auswirken und sich wechselseitig beeinflussen.

2)
Die vergleichende Gesamtbetrachtung der Personenverhältnisse führt zur Feststellung, dass eine pauschale Einordnung von Diensten als Telekommunikationsdienst oder Teledienst nicht gerechtfertigt ist, sondern dass sich diese in Abhängigkeit von den Personenverhältnissen ändern kann. Insbesondere kann auch ein VPN nicht pauschal als geschlossene Benutzergruppe qualifiziert werden, sondern die Einordnung als geschlossene Benutzergruppe muss in Abhängigkeit vom jeweiligen Personenverhältnis beurteilt werden.

3)

Es ist darüber hinaus nicht durchgängig möglich, vom zugrunde liegenden Dienst (z.B. TKG) auf die entsprechenden datenschutzgesetzlichen Regelungen (z.B. §§ 91 ff. TKG) zu schließen. Für die Prüfung von datenschutzrechtlichen Pflichten kann ebenso die Nutzersicht und die Frage entscheidend sein, zu welchem Zweck das VPN verwendet wird bzw. ob eine gemeinsame Zweckverfolgung des VPN-Anbieters und des Nutzers vorliegt. Daraus ergibt sich, dass die jeweilige Leistung eines kombinierten Dienstes (wie einem VPN) mit dem jeweiligen Anbieter und der Zielrichtung des jeweiligen Angebots in Verbindung gebracht werden muss.

4)

Die vergleichende Gesamtbetrachtung der Personenverhältnisse erlaubt die Feststellung, wer die rechtliche Verantwortung für den Betrieb eines Systems (einer Telekommunikationsanlage) innehat und wer dementsprechend der jeweilige Diensteanbieter einer Leistung ist. Die dienstorientierte Betrachtungsweise im Mehrpersonenverhältnis ermöglicht darüber hinaus die Prüfung, inwiefern dem kommerziellen Anbieter des VPN (neben dem Betreiber bzw. VPN-Auftraggeber) eigenständige datenschutzrechtliche Pflichten gegenüber Nutzern und Betroffenen obliegen.

5)

Am Beispiel eines VPN wurde in dieser Arbeit gezeigt, dass die Funktionsherrschaft über ein technisches System (Anlage) nicht gleichzeitig auch die Herrschaft über die auf diesem System stattfindende Datenverarbeitung beinhaltet. Bezüglich der Datenverarbeitung ist zwischen Auftragsdatenverarbeitung und der so genannten Funktionsübertragung zu unterscheiden, wobei die Prüfung in dieser Arbeit ergeben hat, dass letztere aus rechtspolitischen Gründen abzulehnen ist. Im Übrigen führt diese Unterscheidung dazu, dass ebenso ein Auftragsdatenverarbeiter zu staatlichen Auskunfts- und Überwachungsmaßnahmen verpflichtet sein kann.

6)
Im Rahmen von Telearbeit ergibt sich das besondere Problem, dass einerseits die datenschutzrechtlichen Interessen des Nutzers des VPN (Arbeitnehmer) und andererseits des Betroffenen, dessen Daten verarbeitet werden (z.B. Kunden) in Einklang gebracht werden müssen.
Der Betreiber eines VPN muss daher bereits in der Planungsphase eines VPN die unterschiedlichen Interessen von Nutzern (z.B. Arbeitnehmern) und Betroffenen (z.B. Kunden) berücksichtigen, um sowohl die Anforderungen an die Systemsicherheit (im Eigeninteresse) als auch an die Datensicherheit und Datenvermeidung (im Interesse der Nutzer, insbesondere der Arbeitnehmer, und der Betroffenen) sicherstellen zu können.
Im Hinblick auf Arbeitnehmer sind außerdem mögliche Beteiligungsrechte des Betriebsrats zu berücksichtigen.

II. Relevanz der Technik:

1)
Entgegen der häufig vertretenen Meinung können das OSI-Schichtenmodell (als technische Grundlage des Internets und eines VPN) und die so genannten Internet-Dienste (z.B. ftp, Tunneling-Protokolle) keine zuverlässige Aussage im Hinblick auf die rechtliche Einordnung von Diensten als Telekommunikationsdienst oder Teledienst liefern. Im Rahmen der Erbringung eines Telekommunikationsdienstes oder eines Teledienstes können identische Internet-Dienste und damit identische Technik verwendet werden.

2)
Die Untersuchung in dieser Arbeit hat dennoch gezeigt, dass der Technik aber auch erhebliche Relevanz im Rahmen einer rechtlichen Prüfung zukommen kann. Denn als ein Ergebnis wurde festgestellt, dass ein Provider ein Telekommunikationsdiensteanbieter ist, wenn er entweder das Komplettmanagement des VPN oder das Splitmanagement in seinem Machtbereich übernimmt oder die MPLS-Technik verwendet.
Die rechtliche Qualifizierung als Telekommunikationsdiensteanbieter kann damit ebenso von der einer VPN-Leistung zugrunde liegenden Technik und der

VPN-Variante abhängen. Ohne technisches Verständnis ist daher eine juristische Prüfung im Rahmen neuer Online-Dienste nicht möglich.

3)
Die Fortentwicklung der Technik kann zudem dazu führen, dass auch innerhalb eines VPN eine netzseitige Verschlüsselungsmethode in Betracht kommt, die bislang nur für GSM anerkannt wurde. Rechtliche Konsequenz ist, dass staatlich angeordnete Überwachungsmaßnahmen ebenso die Verpflichtung des Diensteanbieters umfassen können, die Verschlüsselung aufzuheben.
Hierbei ist zu berücksichtigen, dass nur Anbieter von Telekommunikationsdiensten staatlichen Auskunfts- und Überwachungsmaßnahmen unterliegen, so dass derjenige, der ein VPN beauftragt, diesen Umstand bei der Entscheidung für eine VPN-Variante („Komplettmanagement durch den Provider") berücksichtigen muss.

4)
Bei der Entscheidung für eine VPN-Variante ist allerdings gleichermaßen die Komplexität der Technik zu beachten, die eine umfassende Aufklärung und Beratung desjenigen erfordert, der ein VPN beauftragt. Allerdings obliegen wiederum ausschließlich Anbietern von Telekommunikationsdiensten gesetzliche Informationspflichten über die Netzsicherheit sowie die Sicherstellung von technischen Schutzmaßnahmen. Daher muss im Einzelfall auf zivilrechtliche Aufklärungspflichten zurückgegriffen werden.

5)
Bei Outsourcing und Telearbeit ist im Rahmen der schutzwürdigen Interessen eines Betroffenen nicht nur die Sicherheit im häuslichen Bereich eines Arbeitnehmers oder im „outgesourcten" Betrieb, sondern gleichermaßen die sichere Übertragung der Daten über das Internet zu berücksichtigen, so dass unter Berücksichtigung moderner Verschlüsselungstechnologien die Anforderungen an die Zulässigkeit von Telearbeit steigen. Aufgrund technischer Innovationen erhöhen sich folglich die Anforderungen, die an das berechtigte und schutzwürdige Interesse des Betroffenen zu stellen sind. Dies gilt insbesondere, sofern die Technik durch die Angebote von unterschiedlichen

Providern weite Verbreitung findet und nicht nur einfach anzuwenden, sondern auch bezahlbar ist. Dies kann im Einzelfall ebenso dazu führen, dass eine Pflicht zur Verschlüsselung der Daten des Betroffenen besteht und die Weitergabe personenbezogener Daten per E-Mail zu unterbleiben hat.

6)
Bezüglich der Nutzer gilt, dass nur die irreversible Datenlöschung auf den technischen Systemen im Sinne einer vollständigen Anonymisierung dem Datenschutz optimal Rechnung tragen kann.

Abschließendes Fazit:

Die in dieser Arbeit dargestellte datenschutzrechtliche Prüfung im Sinne einer wertenden Gesamtbetrachtung der einzelnen Personenverhältnisse bildet die Basis für die Feststellung, wer Diensteanbieter ist und wer Verantwortlicher des Datenschutzes ist. Da die dargestellte Verflechtung mehrerer Personen bei komplexen Dienstleistungen im Internet häufig anzutreffen ist, kann die in dieser Arbeit dargestellte Sichtweise im Übrigen ebenso die datenschutzrechtliche Prüfung und die damit verbundene Einordnung der Dienste im Hinblick auf andere Online-Dienste erleichtern.
Die Zunahme der technischer Komplexität von VPN – oder vergleichbarer, heute noch unbekannnter Online-Dienste – kann darüber hinaus als nahezu gesicherte Entwicklung betrachtet werden. Denn es ist zu berücksichtigen, dass sich der wirtschaftliche Trend der zunehmenden Kommunikation und Arbeitsteilung, stimuliert etwa durch Globalisierung und damit Dezentralisierung, in den letzten Jahrzehnten weder abgeschwächt noch umgekehrt hat. Unter dieser Prämisse werden die hier gewonnenen Ergebnisse bezüglich der Relevanz der Technik und der Relevanz des Mehrpersonenverhältnisses auch für zukünftige VPN oder andere komplexe Online-Dienste juristische und damit ebenso wirtschaftliche Aussagekraft behalten.

In diesem Sinne besteht auch kein Nachbesserungsbedarf im Hinblick auf bestehende oder zukünftige datenschutzgesetzliche Regelungen (etwa des neuen Telemediengesetzes). Daher müssen die Rechte von Betroffenen nicht zusätzlich in einem Datenschutzgesetz geregelt werden, welches sich lediglich auf die Rechtsverhältnisse zwischen einem Diensteanbieter und einem Nutzer bezieht. Der einzige Nachbesserungsbedarf besteht allenfalls im Hinblick auf das Arbeitsrecht, da die Rechte von betroffenen Arbeitnehmern insgesamt besser in einem eigenen „Arbeitnehmerdatenschutzgesetz“ aufgehoben wären.